

AD/A167021

ESD-TR-86-228

MTR-9769

STRATEGIC C³ INTEROPERABILITY EVALUATION:
OPPORTUNITIES AND CHALLENGES

By

P. C. CRANE
M. K. CIMINI

MARCH 1986

Prepared for
DEPUTY FOR DEVELOPMENT PLANS
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
Hanscom Air Force Base, Massachusetts



Approved for Public Release;
distribution unlimited.

Project No. 6250
Prepared by
THE MITRE CORPORATION
Bedford, Massachusetts
Contract No. F19628-84-C-0001

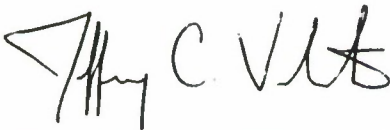
ADA167021

When U.S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Do not return this copy. Retain or destroy.

REVIEW AND APPROVAL

This technical report has been reviewed and is approved for publication.



JEFFREY C. VALITON, Capt, USAF
Chief, Strategic Force Management Division

FOR THE COMMANDER



JOHN G. WHITCOMB, Lt Col, USAF
Director, Strategic C³I Systems Planning

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified			1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release, distribution unlimited.		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE					
4. PERFORMING ORGANIZATION REPORT NUMBER(S) MTR-9769 ESD-TR-86-228			5. MONITORING ORGANIZATION REPORT NUMBER(S)		
6a. NAME OF PERFORMING ORGANIZATION The MITRE Corporation		6b. OFFICE SYMBOL (If applicable)		7a. NAME OF MONITORING ORGANIZATION	
6c. ADDRESS (City, State and ZIP Code) Burlington Road Bedford, MA 01730			7b. ADDRESS (City, State and ZIP Code)		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Deputy for Development Plans		8b. OFFICE SYMBOL (If applicable) XRW		9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER F19628-84-C-0001	
8c. ADDRESS (City, State and ZIP Code) Electronic Systems Division, AFSC Hanscom AFB, MA 01731-5000			10. SOURCE OF FUNDING NOS.		
11. TITLE (Include Security Classification) STRATEGIC C3 INTEROPERABILITY (continued)			PROGRAM ELEMENT NO. 6250		TASK NO. WORK UNIT NO.
12. PERSONAL AUTHOR(S) Crane, P.E.; Cimini, M.K.					
13a. TYPE OF REPORT Final		13b. TIME COVERED FROM TO		14. DATE OF REPORT (Yr., Mo., Day) 1986 March	
15. PAGE COUNT 103					
16. SUPPLEMENTARY NOTATION					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB. GR.	ARPANET Packet-radio		
			Gateway Protocols		
			Interoperability Radio Communications		
19. ABSTRACT (Continue on reverse if necessary and identify by block number) Interoperability can be viewed as a "layered process" in much the same way as protocols are often characterized. Each layer has particular concerns and different possible techniques for dealing with these problems. In this paper the various issues germane to each layer are identified and discussed in light of current military equipment. The issue of "gateway interoperability" is dealt with separately from both a theoretical standpoint and by example.					
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED <input checked="" type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS <input type="checkbox"/>			21. ABSTRACT SECURITY CLASSIFICATION Unclassified		
22a. NAME OF RESPONSIBLE INDIVIDUAL Diana F. Arimento			22b. TELEPHONE NUMBER (Include Area Code) (617)271-7454		22c. OFFICE SYMBOL Mail Stop D230

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

11. EVALUATION: OPPORTUNITIES AND CHALLENGES.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

ACKNOWLEDGMENTS

This document has been prepared by The MITRE Corporation under Project No. 6250, Contract No. F19628-84-C-0001. The contract is sponsored by the Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Massachusetts 01731.

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1.0 INTRODUCTION	1
1.1 An Example	1
1.2 Definitions of Interoperability	8
2.0 INTEROPERABILITY LAYERS	13
2.1 The Equipment Level	13
2.1.1 HF Equipment	14
2.1.2 VHF Equipment	14
2.1.3 UHF Microwave and Troposcatter Equipment	23
2.1.4 General Observations Concerning Equipment	25
Level Protocols	
2.2 The System Layer	25
2.2.1 Message Formats	26
2.2.2 Network Control and Access	27
2.2.3 Alphabets	27
2.2.4 Timing	28
2.2.5 General Observations Concerning System	28
Level Protocols	

TABLE OF CONTENTS (CONTINUED)

<u>SECTION</u>	<u>PAGE</u>
2.3 The Operational (Organizational) Layer	30
2.3.1 HF Operational Level Interoperability	30
3.0 GATEWAY INTEROPERABILITY	41
3.1 Characteristics of the ARPANET	41
3.2 Characteristics of a PRNET	46
3.3 Protocols and Interfaces - General Concepts	50
3.4 ARPANET Protocols	54
3.4.1 The TELNET Protocol	58
3.4.2 The Transmission Control Protocol (TCP)	62
3.5 Interconnecting Networks via Gateways	63
3.5.1 Interconnect Level	64
3.5.2 Type of Service	65
3.5.3 Addressing	66
3.5.4 Routing	66
3.5.5 Segmentation/Collection	67
3.5.6 Flow Control	67
3.5.7 Reliability	68
3.5.8 Security	68
3.5.9 Broadcast Support	68
3.5.10 Gateway Hardware Characteristics	69
3.5.11 BB Connection to a Host-BB Appears as a Terminal	69
3.5.12 BB Connection to a TAC-BB Appears as a Terminal	71

TABLE OF CONTENTS (CONCLUDED)

<u>SECTION</u>	<u>PAGE</u>
3.5.13 BB Appears as a Host	72
3.6 Conclusions Regarding an HF/ARPANET/PRNET Interface	72
3.6.1 HF Interface to PRNET	74
3.6.2 HF Interface to the ARPANET	74
3.6.3 HF Gateway Characteristics	75
3.6.4 Cryptographic Considerations	78
4.0 CRYPTOGRAPHIC ASPECTS	79
4.1 Intra-Crypto-Net Communication	79
4.1.1 Key Management	80
4.1.2 Overhead	81
4.1.3 RED/BLACK Isolation	83
4.2 Inter-Crypto-Net Communication	84
4.2.1 Key Management	84
4.2.2 Overhead	84
4.2.3 RED/BLACK Isolation	85
5.0 COMPATIBILITY	87
REFERENCES	89
GLOSSARY	91

LIST OF ILLUSTRATIONS

<u>FIGURE</u>		<u>PAGE</u>
1.1	ARPANET Geographic Map, 31 December 1984	2
1.2	MILNET Geographic Map, 31 December 1984	3
1.3	SACDIN Nodes (Projected 1987)	4
1.4	GWEN FOC Relay Nodes	5
1.5	Interoperability Example	7
1.6	Interoperability Layers	10
3.1	ISO Reference Model for Open Systems	52
3.2	ARPANET Protocols and Interfaces	55
3.3	Further Details on ARPANET Protocols and Interfaces	56
3.4	HF/ARPANET Interface Considerations	73

LIST OF TABLES

<u>TABLE</u>		<u>PAGE</u>
2.1	HF Equipment Characteristics	15
2.2	VHF Equipment Characteristics	18
2.3	Troposcatter Equipment Characteristics	24
2.4	SAC HF Requirements	31
2.5	MAC HF Requirements	32
2.6	TAC HF Requirements	33
2.7	AF COMM COM HF Requirements	34
2.8	AFLC HF Requirements	35
2.9	ADCOM HF Requirements	36
2.10	ESC HF Requirements	37
2.11	USAFE HF Requirements	38
2.12	PACAF HF Requirements	39
3.1	Experimental Packet Radio Characteristics	48

1.0 INTRODUCTION

There is a growing clamor in the military communications community for "interoperability". It is generally conceded that interoperability will result in increased convenience, compatibility, efficiency of command and control and reduced costs. The enhanced connectivity of Air Force communications achieved by the interconnections of various networks should also result in greater communications survivability through the route redundancy and flexibility obtained by this interconnection.

1.1 An Example

As an example of the coverage and connectivity that could be achieved, consider figures 1.1 through 1.4. Figure 1.1 is a map of the Advanced Research Projects Agency Network (ARPANET) as of 31 December 1984. Figure 1.2 is a map of the Military Network (MILNET) as of the same date. The ARPANET and MILNET are both components of the Defense Data Network (DDN) and much work has been, and will continue to be, done on gateways involving these networks. Figure 1.3 shows the Strategic Air Command Digital Network (SACDIN) as it is projected for 1987. Figure 1.4 depicts the Groundwave Emergency Network (GWEN) Final Operational Capability (FOC) relay node network. Packet Radio Network (PRNET) has already been successfully interfaced to the ARPANET and has been shown to be capable of reconstituting a severed ARPANET. This capability could probably be extended to generic networks by developing suitable interfaces. Taking this entire collection of the four networks, local PRNETs, MILSTAR, and HF one could easily envision a super network composed of the above components melded together by a system of gateways.

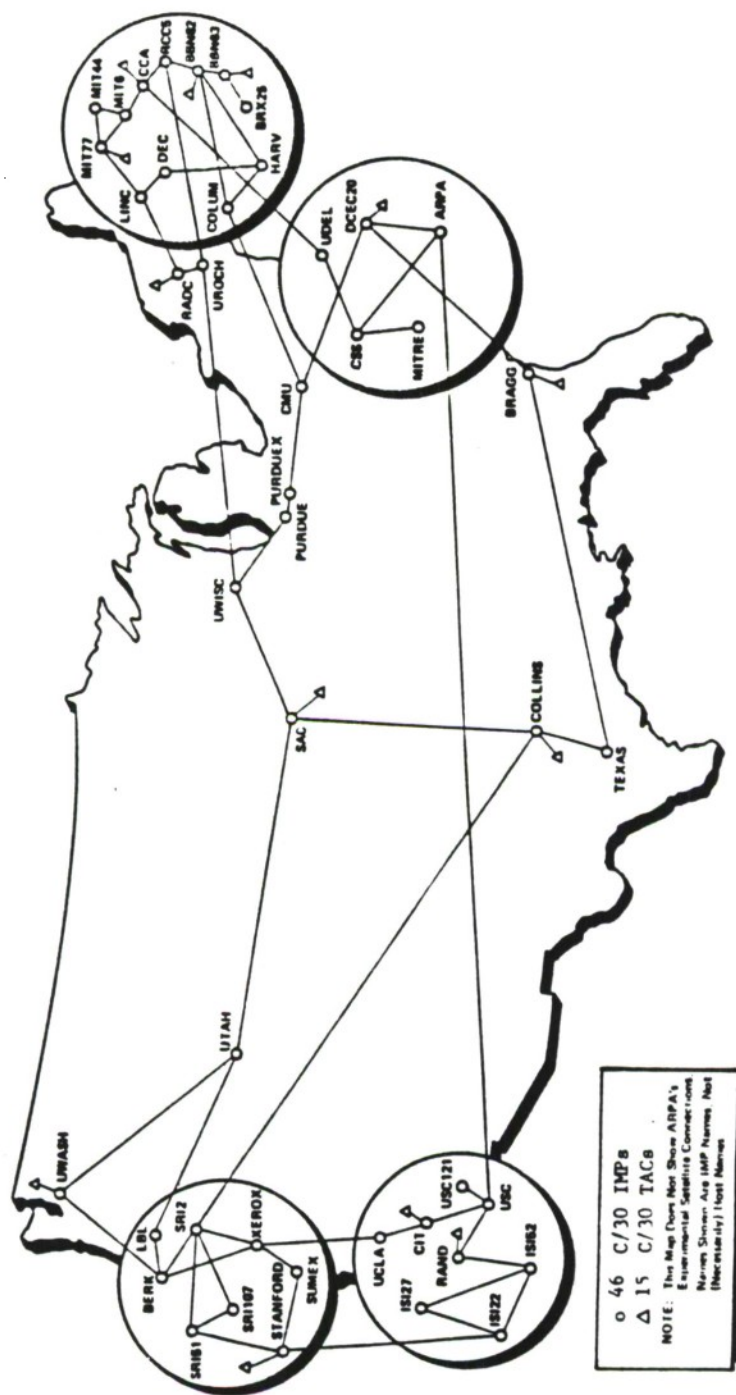


Figure 1.1. ARPANET Geographic Map, 31 December 1984



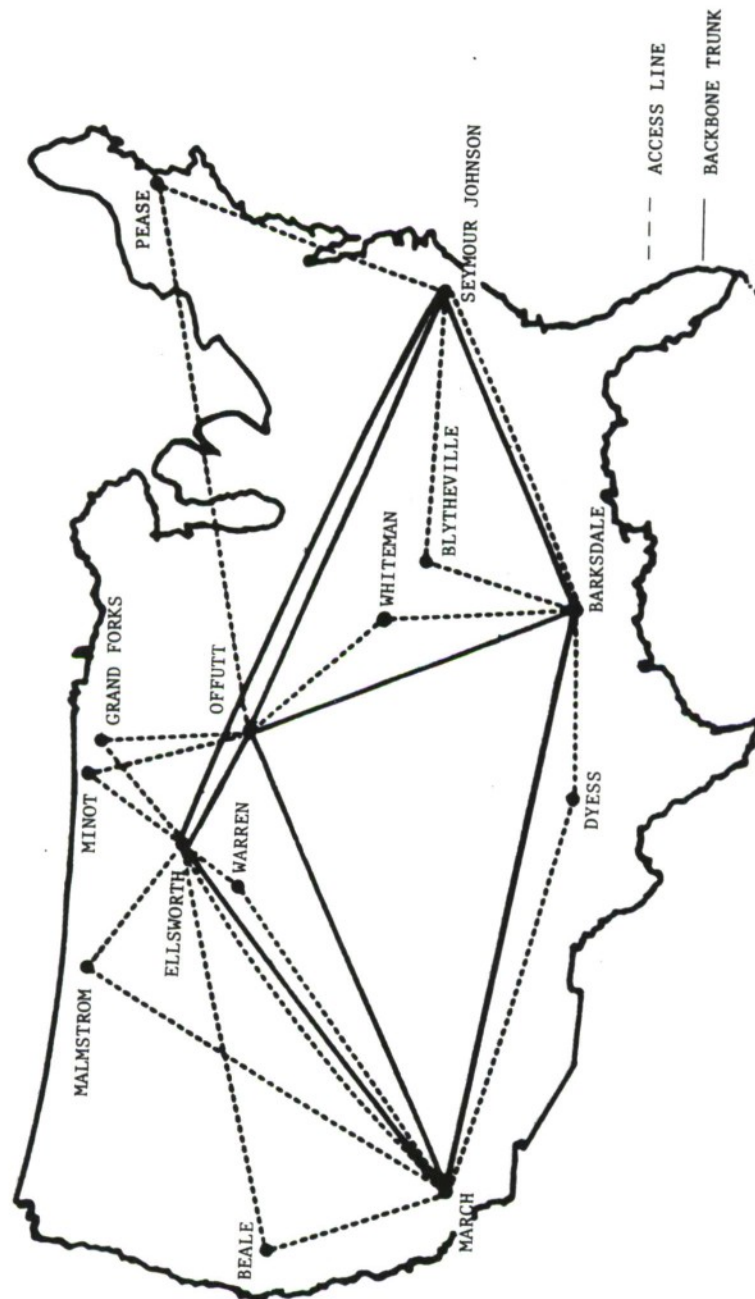


Figure 1.3. SACDIN Nodes (Projected 1987)

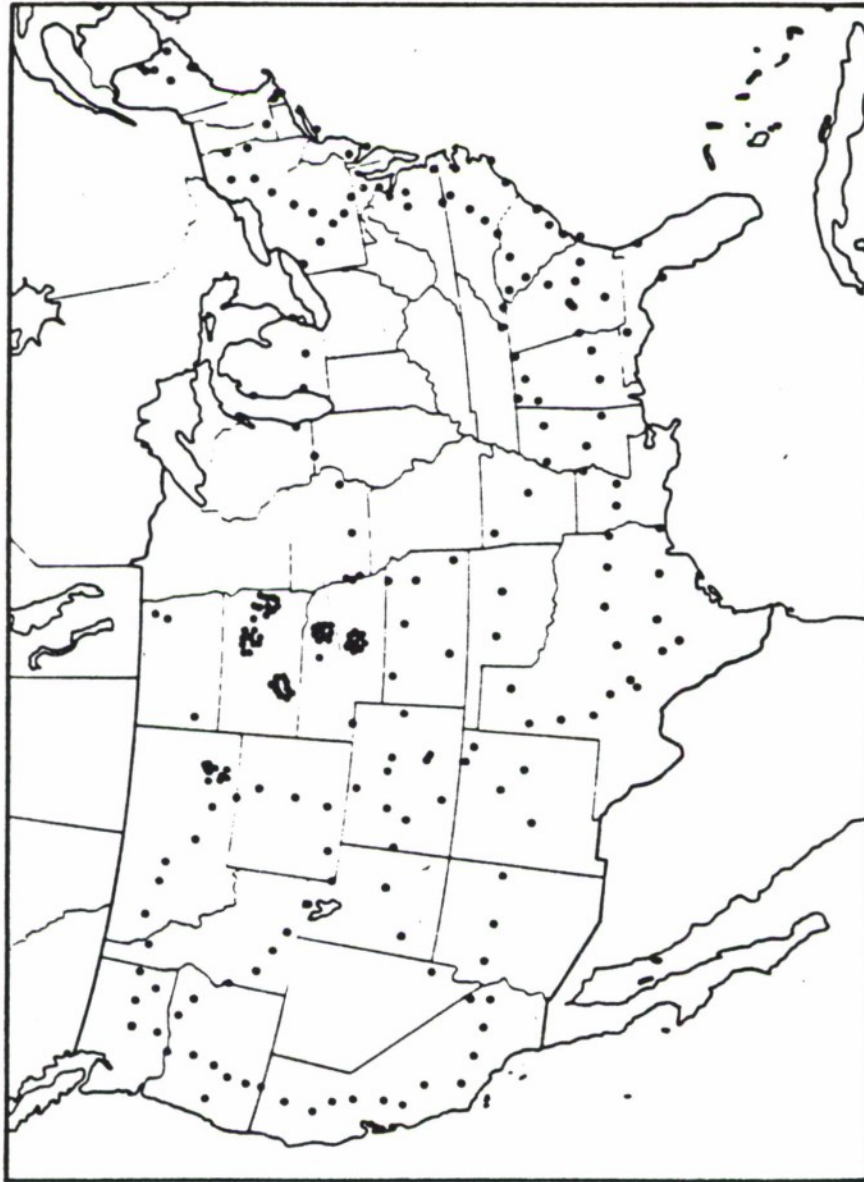


Figure 1.4. GWEN FOC Relay Nodes

The benefits of such a conglomerate are fairly obvious but let us consider an example (Figure 1.5) of how things could work. Suppose that in the post-attack world the limited access of GWEN is relaxed so as to allow returning bombers to use intact segments of GWEN as injection nodes into a large interconnected system composed of surviving communications assets. A returning bomber could then enter GWEN by UHF, the message would then be sent along the GWEN network until a disconnect is encountered whereupon the message would pass through an automatic gateway into an HF network. It may then be that the HF radio is only capable of establishing a link to a small number of nodes. Suppose one of these nodes has a MILSTAR terminal. The message would then pass through another gateway into the MILSTAR system. MILSTAR may be incapable of delivering the message to the intended destination, but suppose it can reach an ARPANET node. The message would then trickle through the ARPANET until it reaches a disconnect in the ARPANET. This disconnect could be bridged by PRNET and we shall suppose this happens. However let us suppose the ARPANET is sufficiently disrupted so that SAQ HQ still cannot be reached. The message could then pass through an ARPANET/HF gateway and is finally delivered to SAC HQ via HF.

Conversely, the above route could be used in reverse by SAC HQ to distribute landing field data to the returning bombers.

We realize that much of the technology (i.e. interfaces and other support equipment) needed for the above route does not currently exist. We also realize that there are protocol and security problems with the above example. The example is intended as an illustration of things that are, at present, only conceptual. It is hoped however that the value of technology of this sort is realized.

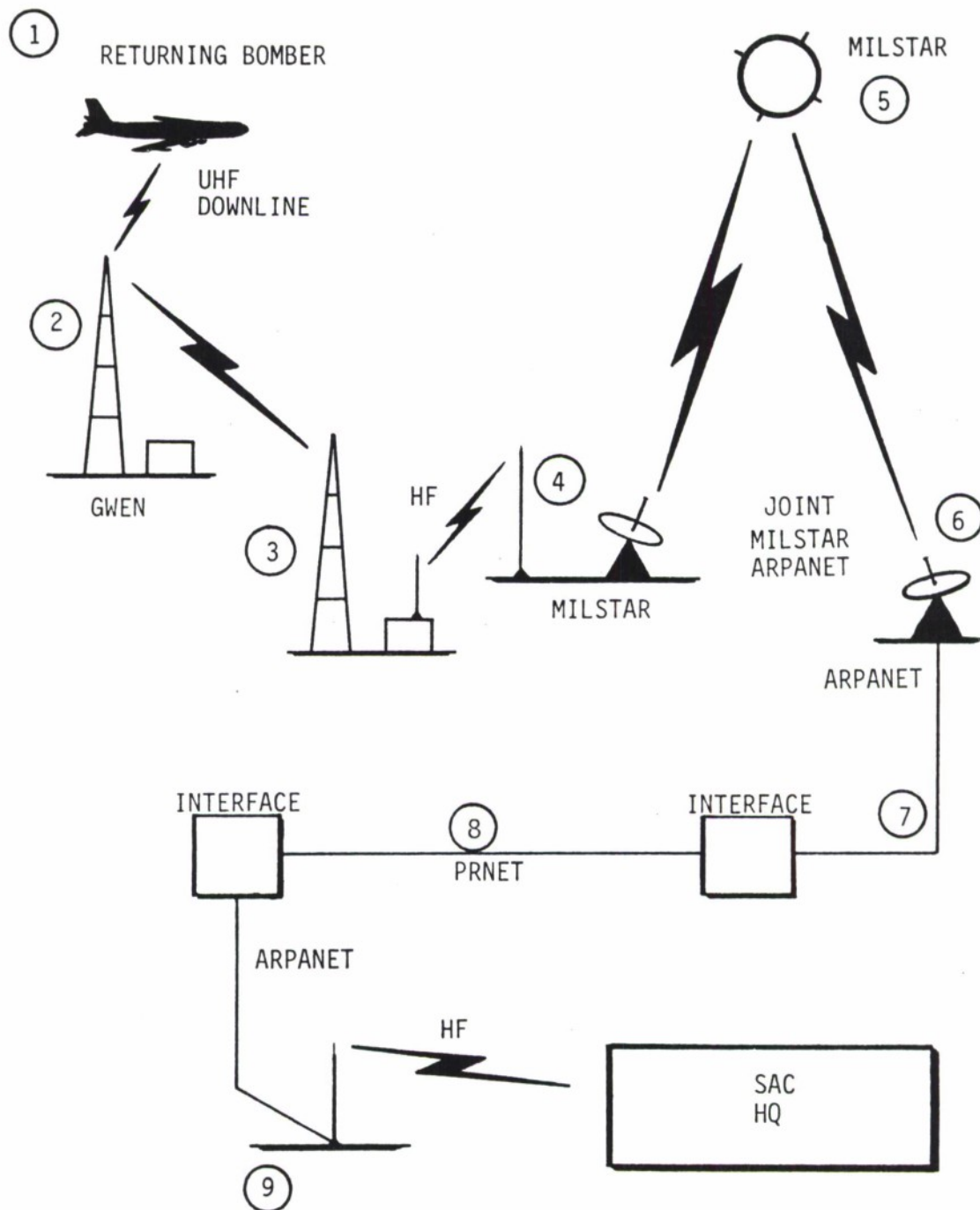


Figure 1.5. Interoperability Example

1.2 Definitions of Interoperability

All the various definitions and/or explanations of the term have the following common theme: If entity A (it could be an organization, a network, a location, a soldier, etc.) can use its communications equipment to quickly and easily pass information to entity B via entity B's communications equipment, then, in some sense at least, entity A's communications equipment (or perhaps system) is interoperable with entity B's communications equipment (system). This could involve merely tuning similar equipment to the same mode and frequency or it could involve the use of rather esoteric automatic gateways between dissimilar networks.

Interoperability is defined in various ways depending upon the criteria deemed important by the parties involved. It may or may not involve automatic information interchange. It can refer to the interoperation of similar equipment on a common communications network or it can refer to the rapid and effective exchange of communications between entities in completely different organizations, accomplished by a "meshing" of their various communications assets. The following are the interoperability definitions of the FCC, DoD, and NSDD.

FCC - The capability of radio/electronic equipment under the control of one entity to interconnect (send or receive communications) with equipment controlled by others.

DoD - The condition achieved among communications-electronics systems when information or services can be exchanged directly and satisfactorily between them and/or their users.

NSDD - The ability of functionally similar networks to rapidly and automatically interchange traffic.

In this report we shall view interoperability as a three layer process. There will be various factors of interest at each layer and lower layer concerns should be invisible to higher layers. Figure 1.6 depicts this approach.

Organizational (i.e., operational) interoperability could also be accomplished by the use of "gateways" allowing dissimilar equipment in different communications networks to gain access to a desired network through such a device. This issue will be dealt with in Section 3.

The most basic form of interoperability is achieved by using communications equipment of some common type to pass simple, uncontrolled traffic. This involves no more than setting the equipment at both ends to a common set of parameters and attempting to establish a link. If some form of network access and/or flow control is in effect, the problem becomes more complicated. If modems, printers, docoders, etc. are also required, then the problem becomes one of total system commonality and not simply one of tuning similar radios.

Some of the advantages accrued from what we shall dub "system commonality" are as follows:

1. Improved area and/or organizational coverage due to "merging" networks of similar equipment.

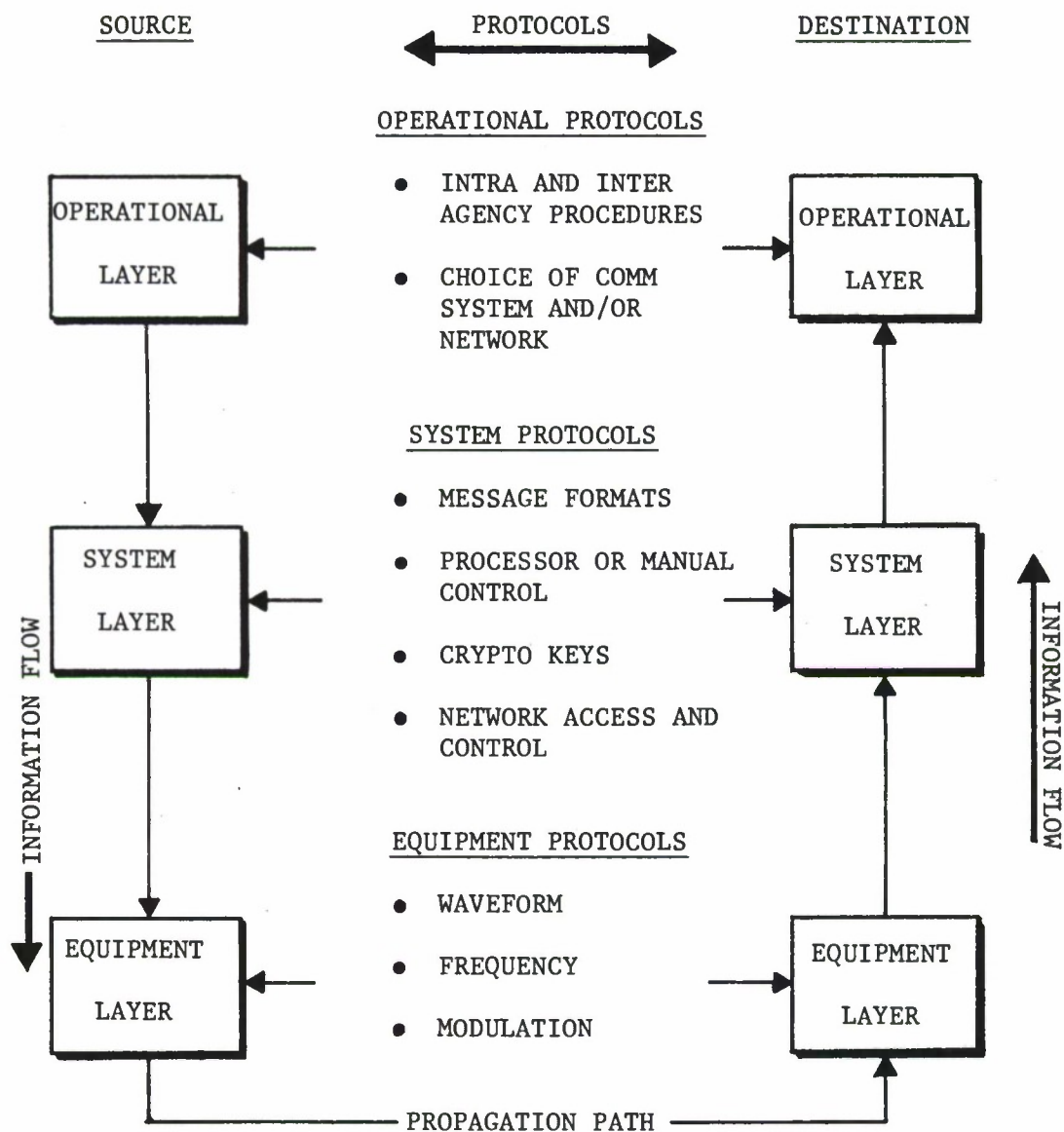


Figure 1.6. Interoperability Layers

2. Improved connectivity in a given network achieved by temporarily "adding nodes" from another similar interoperable network(s) to the given network or by using the other interoperable network(s) to obtain redundant communications paths.
3. The increased ability to "repair by replacement" by "pirating" networks and/or nodes of some lesser importance.
4. Simplicity (from the operator standpoint). That is, less training may be necessary if more equipment had similar operational characteristics.
5. Possible reductions in the amount of equipment needed at the unit level.

Some examples of interoperating networks, where the interoperability is due to system commonality, are the 616A/VERDIN/IRR LF systems and certain HF networks operated by various government and DoD agencies. Some of these HF nets and resulting interoperability are as follows:

1. Army/Air Force/Navy
2. Air Force/FAA
3. Air Force/VA

4. Navy/Coast Guard
5. FEMA/VA
6. FAA/Coast Guard/Customs/DEA
7. Dept. of Energy/Dept. of Interior

It may be that interoperability is desired among two or more entities that do not possess communications equipment of sufficient similarity so as to enable a link to be established. In such a case the entities would need to be connected via a "gateway".

A gateway is a device that is capable of receiving a message from entity A, transforming the message into a form acceptable to entity B, and sending the message to entity B. This gateway could be a set of transceivers (as well as modems, coders, etc.) controlled by a computer so as to accomplish the gateway function automatically or it could be a radioman with a pencil and paper.

The advantages of "gateway interoperability" are these:

1. Allows a greater variety of networks and/or locations to be interconnected resulting in greatly improved area coverage and connectivity.
2. Allows resource sharing, particularly among computer networks.
3. Permits possible reductions in equipment and possibly greater operator simplicity at the unit level.

Some examples of gateway interoperability are the ARPANET/PRNET system currently being investigated by SAC and the various interconnected computer networks that comprise the DDN.

2.0 INTEROPERABILITY LAYERS

In this section we shall discuss the relevant issues of each interoperability layer. These issues will be defined in terms of protocols to be followed in order to establish virtual communications between corresponding layers within the source and destination entities. By virtual communications it is meant that, for example, a system level communicator at the source entity would seem to be in direct communication with a system level communicator at the destination entity. The actual flow of information would go down to the equipment level and through the propagation path, etc. The system level communicators would be in touch with their respective operational and equipment levels but would be unconcerned with the issues particular to these levels.

2.1 The Equipment Level

Equipment level protocols require that the candidate equipment be tunable to a common frequency and use a common waveform and modulation technique. That is, these protocols specify what characteristics the equipment must have in order to communicate at all with the other candidate equipment.

The remainder of this subsection gives specific information pertinent to equipment level interoperability for a variety of military communications equipment.

2.1.1 HF Equipment

Table 2.1 lists the relevant characteristics of some of the HF equipment now in use by various defense organizations. All of this equipment can interoperate in at least one mode over some portion of the HF spectrum. The more capable equipment can interoperate using both voice and data. It seems safe to conclude that equipment level protocols should not be a serious obstacle to interoperability at HF.

Most of the HF equipment listed as operable using FSK and FAX require external modems to accomplish this. There are also a large number of high capability fixed site HF radios that are not included. They are all interoperable, generally over all of the HF band.

2.1.2 VHF Equipment

Table 2.2 gives information on VHF equipment. It appears that the AN/GRC-206, AN/TRC-176, AN/PRC-70, AN/URC-104, AN/VRC-12, AN/VRC-64, AN/VRC-43 to 49, AN/GRC-160, AN/ARC-54, AN/ARC-114A, AN/ARC-131, AN/ARC-182, MIL-7854, ERC-310, ERC-320, AN/PRC-68, AN/PRC-77 and the AN/PRC-99 will all interoperate using FM over portions of the lower VHF band. The AN/GRC-206, AN/TRC-176, AN/VRC-83, AN/ARC-73A, AN/ARC-84, AN/ARC-101, AN/ARC-182, AN/ARC-186, AN/ARC-195, AN/PRC-106, RC-113, AN/PRC-113, AN/URC-100 and AN/URC-101 will interoperate using AM in the middle portion of the VHF band. At the upper end of the band inoperability can be achieved using AM by the AN/VRC-83, RC-113, RC-130, AN/ARC-109, RT-1017/ARC, AN/ARC-159, RT-1194/ARC-159A, RT-1150/ARC-159,

TABLE 2.1
HF EQUIPMENT CHARACTERISTICS

<u>EQUIPMENT</u>	<u>HF FREQ. RANGE (MHz)</u>	<u>MODULATIONS AND OPERATING MODES</u>
AN/GRC-106A	2-30	FSK, CW, (USB, AM while transmitting) (DSB, AM while receiving), (voice and data)
AN/MRC-138 AN/GRC-193	2-30	FSK, USB, LSB (voice, TTY, or data)
AN/GRC-206	2-30	USB, LSB (voice)
AN/GRC-213	2-30	SSB (voice)
AN/PRC-15	2-30	LSB, USB, AM, CW (voice)
AN/PRC-70	2-30 (Range extends to 76)	USB, AM, CW, FSK
AN/PRC-74B	2-18	SSB, CW (voice)
AN/PRC-104	2-30	SSB (voice)
AN/URC-79	2-30 (Range extends to 1.6)	SSB, CW, FSK (voice or data)

TABLE 2.1 (Continued)

<u>EQUIPMENT</u>	<u>HR FREQ. RANGE (MHz)</u>	<u>MODULATIONS AND OPERATING MODES</u>
AN/URC-87	2-12	USB, LSB, CW, AM (voice)
AN/URC-94	2-30 (Full range is 1.5-8.0)	AM, LSB, USB, CW, FM, FSK, FAX (voice or data)
AN/URC-106	2-30 (Range extends to 1.6)	LSB, USB, AME, CW, FSK, FAX (voice and data)
AN/URR-69	2-30 (Range extends to 0.5)	AM, FM, CW/FSK, USB, LSB (voice)
HF-80	2-30	USB, LSB, AME, CW, ISB (voice and data)
HF-120	2-30	USB, LSB, AME, CW, FSK (voice and data)
HF-125	2-30	USB, LSB, AME, CW (voice, line input for data)
AN/ARC-98	2-30	USB, LSB, AME, (VOICE); USB, ISB (data)
AN/ARC-153	2-30	USB, LSB, ISB, AME (voice and data)

TABLE 2.1 (Concluded)

<u>EQUIPMENT</u>	<u>HF FREQ. RANGE (MHz)</u>	<u>MODULATIONS AND OPERATING MODES</u>
AN/ARC-157	2-30	USB, LSB (voice and data)
AN/ARC-161	2-30	USB, LSB, AFSK (voice, TTY and data)
AN/ARC-174	2-30	USB, LSB, AME, CW, SVU, SVL, (voice and data)
AN/ARC-190	2-30	USB, LSB, AME, CW, AFSK (voice and data)
AN/ARC-191 AN/ARC-512	2-30	USB, LSB, LSB, AME (voice and data)

TABLE 2.2
VHF EQUIPMENT CHARACTERISTICS

<u>EQUIPMENT</u>	<u>VHF FREQ. RANGE (MHz)</u>	<u>MODULATIONS AND OPERATING MODES</u>
AN/TRC-206	30-75.95** 116-149.975	FM AM (FM available on request)
AN/TRC-176	225-300*	AM (FM available on request)
AN/PRC-70	30-76*	USB, AM, CW, FSK, FM
AN/URC-104	30-88 225-300*	AM, FM voice, cipher text and emergency beacon
AN/VRC-12		
AN/VRC-64		
AN/VRC-43 to 49	30-75.95	FM (voice)
AN/GRC-160		
AN/VRC-83	116-150 225-300*	AM (voice)
SINCGARS V	30-88	FM, AM option possible single channel frequency hopper, data retransmission
MIL-7854	36-41.5	FM (voice)

*Range actually extends into the UHF band (to 400 MHz)

**Range extends into HF band (to 2 MHz)

TABLE 2.2 (Continued)

<u>EQUIPMENT</u>	<u>VHF FREQ. RANGE (MHz)</u>	<u>MODULATIONS AND OPERATING MODES</u>
ERC-310 ERC-320	30-80	FM (voice)
RC-113	116-150 225-300*	AM voice, DF tone data TSEC/KY-57, TSEC/KY-58
RC-130	225-300*	AM voice, AM wideband data (16 kb/s diphase)
AN/PRC-66B	225-300*	AM (voice)
AN/PRC-68	30-79.95	FM (voice)
AN/PRC-77	30-75.95	FM (voice)
AN/PRC-94	132-174	FM (voice)
AN/PRC-99	30-80	FM (voice)
AN/PRC-112	121.5 225-299.975	Swept tone beacon AM (voice)
AM/PRC-113	116-150 225-300*	AM (voice)

*Range actually extends into the UHF band (to 400 MHz)

TABLE 2.2 (Continued)

<u>EQUIPMENT</u>	<u>VHF FREQ. RANGE</u> <u>(MHz)</u>	<u>MODULATIONS</u> <u>AND OPERATING MODES</u>
AN/PRC-117	30-89.975	Frequency hopper, narrow band voice, wide band data (to 16 kb/s), data retransmit
AN/URC-100	116-150	AM, FM (voice); AM cipher text
AN/URC-101	225-300*	AM or FM voice; AM or FM cipher text AM or FM emergency beacon
AN/URC-94	30-80**	AM, LSB, USB, CW, FM, FSK, FAX
AN/ARC-54	30-95	FM (voice)
AN/ARC-73A	116-149.95	AM (voice)
AN/ARC-84	118-136	AM (voice)
AN/ARC-101	116-150	AM (voice)
AN/ARC-109	225-300*	AM (voice)
AN/ARC-114A	30-75.95	FM (voice)
AN/ARC-131	30-75.95	FM (voice)

*Range actually extends into the UHF band (to 400 MHz)

**Range extends into HF band (to 2 MHz)

TABLE 2.2 (Continued)

<u>EQUIPMENT</u>	<u>VHF FREQ. RANGE (MHz)</u>	<u>MODULATIONS AND OPERATING MODES</u>
RT-1017/ARC	225-300*	AM, FM (voice and secure voice)
AN/ARC-159	225-300*	AM (voice and data)
RT-1194/ARC- 159A	225-300*	AM (voice and secure voice)
RT-1150/ARC- 159		
AN/ARC-164	225-300*	AM, FM voice; FSK data
AN/ARC-171	225-300*	AM voice and secure voice, FM voice and data, FSK
AN/ARC-182	30-88	FM
	108-156	AM
	156-174	FM (voice)
	225-300*	AM, FM
AN/ARC-186/	30-87.975	FM (voice and secure voice)
VHF-186	108-155.987	AM (voice and secure voice)
AN/ARC-187	225-300**	AM (voice and secure voice), FM/FSK data

*Range extends into UHF band (to 400 MHz)

**Range extends into UHF band

TABLE 2.2 (Concluded)

<u>EQUIPMENT</u>	<u>VHF FREQ. RANGE</u> <u>(MHz)</u>	<u>MODULATIONS</u> <u>AND OPERATING MODES</u>
AN/ARC-195	100-160	AM (voice and secure voice)
AN/APR-69	225-284.9	AM (voice, automatic direction finding)
AN/PRC-106	121.5 and 243	AM (voice, Emergency beacon)

AN/ARC-164, AN/ARC-171, AN/ARC-182, AN/ARC-187, AN/ARC-69, AN/PAC-106, AN/PRC-66B, AN/PRC-112, AN/PRC-113, AN/URC-100 and AN/URC-101. In addition, the AN/ARC-164, AN/ARC-182, AN/URC-100, AN/URC-101, RT-1017/ARC and AN/ARC-187 can interoperate at the upper end of the band using FM. The AN/PRC-94 is only able to interoperate with the AN/URC-100, AN/URC-101, AN/URC-102 and some AN/GRC-206s and AN/TRC-176s using FM in the mid-VHF band.

While this equipment level interoperability at VHF does not seem quite as ubiquitous as at HF a considerable degree of interoperability exists.

2.1.3 UHF Microwave and Troposcatter Equipment

A considerable number of HF/VHF communication equipment extend their operational frequency ranges into the lower UHF band. In particular the AN/GRC-206, AN/TRC-176, AN/URC-104, AN/VRC-83, RC-113, RC-130, AN/ARC-66B, AN/PRC-113, AN/URC-100, AN/URC-101, AN/ARC-109, RT-1017/ARC, AN/ARC-159, RT-1194/ARC-159A, RT-1150/ARC-159, AN/ARC-164, AN/ARC-71, AN/ARC-182 and AN/ARC-187 all extend their ranges to about 400 MHz. Most use AM in this range but some are able to use FM. The above equipment will or will not interoperate as described in Section 2.1.2.

Table 2.3 gives data on some troposcatter equipment. In general, this equipment can be configured so as to interoperate. The question is whether interoperability is an important issue for microwave and troposcatter equipment. The location of the parties wishing to communicate must be known to each other to a fairly precise degree. This negates at least one of the reasons for

TABLE 2.3

TROPOSCATTER EQUIPMENT CHARACTERISTICS

<u>EQUIPMENT</u>	<u>FREQ. RANGE</u>	<u>MODULATIONS AND OPERATING MODES</u>
AN/GRC-201	4.4-5 GHz	FM (voice, TTY (FSK), data) FDM or PCM (12 or 24 channels) 16 TTY channels per voice channel
AN/TRC-97	4.4-5 GHz	FM (voice TTY (FSK), data) FDM (12 or 24 channels) 16 TTY channel per voice channel
AN/GRC-143	4.4-5 GHz	FM PCM (12 or 24 channels) 15 or 30 channel data modulation also available
AN/GRC-144	4.4-5 GHz	FM PCM (48 or 96 channels)

interoperability; that is, the reconstruction of a communications network using whatever has survived a nuclear attack. In the confusion following an attack it is doubtful that this sort of equipment could make significant contributions to a general communications network. UHF interoperability is probably a more important issue as it is used for air control.

2.1.4 General Observations Concerning Equipment Level Protocols

Equipment level protocols are absolutely essential if any communications at all are to take place. They are also the best understood and most easily implemented. It is usually a fairly easy matter to establish equipment level communications as long as the source and destination are within communications range of each other, have equipment that can operate in the desired mode, and can tune to a common frequency. This assumes that both nodes know when the communication is to occur and, if necessary, the location of the other node. Schedules and knowledge of nodal locations are part of the network access procedures, however, and are not equipment level concerns.

2.2 The System Layer

System layer protocols are concerned with issues affecting the operation and control of the network given that the communications equipment possess sufficient commonality to enable information to be exchanged at all. Things like message formats, processor or manual control of the communications equipment, crypto keys, network access techniques, central or distributed network control, alphabets and timing considerations are system layer protocols.

2.2.1 Message Formats

In order for a received message to be understood (especially a non-voice message) the destination must be aware of the format used by the source. Messages are structured in such a way as to allow particular bit streams, which may or may not be located in particular fields in the message, to accomplish such things as printer carriage control, modem control, synchronization, error control, Automatic Repeat ReQuest (ARQ), mode selection, message repeat, and many other functions.

It may be necessary to perform bit stuffing (i.e. the addition of extra bits into a particular group of bits) at either or both the source and destination to avoid the unintentional creation of some unwanted bit stream which could, for example, turn off the receiving nodes modem in mid-message. Naturally, if this technique is employed at the transmitting node the procedure must be known to the receiving node.

A technique related to bit stuffing is the use of forward error correction codes. Extra bits are added to groups of information bits for the purpose of the detection and correction of errors introduced into the information bits during the process of transmission and reception. Such codes are normally implemented by the system's hardware (i.e., shift registers), and both the source and destination must be using the same code.

Forward error correction codes may be augmented by the use of an ARQ technique, should an uncorrected error be detected. Error detection is normally accomplished either by a forward error

correction code or by a Cyclic Redundancy Check (CRC). When a CRC is used, additional CRC bits are added to the message before transmission. The pattern formed by the CRC bits is a function of the totality of the message bits and the construction of this pattern is usually accomplished via system hardware. At the receiving end the message is again subjected to the creation of the CRC bit pattern (after error correction has occurred if error correction codes are being used) and this newly created pattern is compared to the CRC pattern added to the message at the transmitting end. The two patterns must coincide. If they do not, then the message contains an uncorrected error and an ARQ is sent. This technique can be used by itself or in conjunction with forward error correction. In any event the CRC procedure must be common at both the transmitting site and the receiving site.

2.2.2 Network Control and Access

Any entity wishing to interoperate with a communications network must observe that networks methods for message traffic control and channel access. This would involve the ability to communicate with a network control node or the ability to implement distributed control procedures. In order to access the networks communications channels, the node might, for example, be required to keep accurate time (for TDMA), be required to be able to operate at a variety of network frequencies (FDMA) or have knowledge of the proper PN code (CDMA).

2.2.3 Alphabets

There are actually two different types of alphabets that must be considered; the character alphabet formed by bit patterns and the symbol alphabet used in M-ary techniques. Both must coincide (provided of course that M-ary signalling is in use).

2.2.4 Timing

Timing considerations vary as the type of equipment and method of network operation. For TDMA operation, some degree of synchronization is required to even access the network. For some types of systems the allowable communications range can be limited by the width of the receiver's synchronization window. For any sort of frequency hopping or PN modulation, timing is important.

2.2.5 General Observations Concerning System Level Protocols

System level protocols are normally quite specific functions of system design and operation. It is quite easy to proclaim two systems to be interoperable and to completely miss some critical factor that will negate the expected interoperability. Some experimentation is almost always required in order to configure an existing system so as to interoperate with another existing system. By way of example, let us consider a DCA/CCEC program to verify interoperability between the USAF 616A, the USN VERDIN, and the USN Integrated Radio Room (IRR) VLF/LF communications systems of the Minimum Essential Emergency Communications Network (MEECN).

The 616A system is comprised of the AN/ARC-96 in the NEACP and WWABNCP aircraft, the AN/FRC-117 at Hawes, Silver Creek and the ANMCC, the AN/FRR-97 at the LCC installations, the AN/FRC-97/98 at

other ground sites and the AN/TRR-34 at CINCUSAREUR and EUNIEF. The VERDIN system uses the AN/USC-13 at TACAMO installations and the AN/WRR-7 at submarine installations. The IRR system is used by the TRIDENT submarines.

The 616A, VERDIN, and IRR systems are interoperable at the equipment level and are designed to be compatible at the system level in the MEECN modes. The VERDIN and IRR systems are software-based while the 616A system is hardware-based. This dissimilarity in design philosophy was one of the areas of concern regarding system level interoperability. Other concerns were cryptographic compatibility, timing considerations and format structure.

An example of an interoperability problem, which was discovered experimentally, is the structure of the end-of-message indicator. It was originally thought that "NNNN" would be adequate for this task. It turned out that this pattern switched the 616A modulator to the idle mode. "Line feed NNN" was tried and this pattern was found to turn off the power to the 616A printer. Finally, "line feed NNNN" was found to work.

Another example was the failure to remove a field of K's from the format. It turns out that this pattern will allow only clear text to be used.

These problems could have been found by careful perusal of the appropriate technical documents. However, this sort of thing is easily missed and experimentation is necessary in order to remove all such system "bugs".

2.3 The Operational (Organizational) Layer

Operational layer protocols are concerned with issues such as the appropriate "address" within a given organization to which a particular message should be sent, what communications media should be used and what procedures should be followed in establishing such communications.

Operational layer protocols are commonly exercised in a "second-nature" fashion by nearly every defense organization. For example the postal service employs operational layer protocols to deliver mail. Probably the difficulty from a technical standpoint is determining how to automate such procedures.

While this sort of communications is widely used, there appears to be rather scanty documentation as to type and volume. A study on Inter-service HF interoperability is summarized in the next subsection. The study provides some feel for the issues involved in the operational layer of interoperability.

2.3.1 HF Operational Level Interoperability

Due to the wide proliferation, relatively low cost, degree of commonality and long communications ranges characteristic of HF radio, this equipment is frequently used for inter-service and inter-organizational (within a specific service or agency) communications. Tables 2.4 through 2.12 show the type of traffic carried and the entities required to interoperate with various AF organizations via that traffic at HF. The traffic parameters are for all HF traffic involving that organization and not just the

TABLE 2.4
SAC HF REQUIREMENTS

	<u>SYSTEM APPLICATION</u>	
	<u>EAM DISSEMINATION</u>	<u>OTHER GROUND-AIR-GROUND</u>
<u>INFORMATION TYPES</u>		
VOICE	Secure, AJ	Secure, AJ
TTY (<300 wpm)	Secure, AJ	Secure, AJ
DATA (>300 wpm)	-----	-----
<u>TRAFFIC PARAMETERS</u>		
MESSAGE LENGTH	200 Characters	10-1000 Words
LOADING	-----	-----
TYPE		
Point to Point	Limited	All Apply
Group	Moderate	
Broadcast	Primary	
TERMINAL TYPE/NUMBER		
Airborne	≈1200	≈1200
Ground Fixed	≈ 200	≈ 200
Ground Mobile	≈ 30	≈ 30
<u>TIMELINESS</u>	20 Min. Authenticated	Minutes Connectivity
<u>SECURITY</u>	Yes	Yes
<u>INTEROPERABILITY</u>		
INTRA AIR FORCE	USAFE, PACAF	Limited
INTER SERVICE	Yes	Limited
NATO	Limited	Limited
CANADA	Limited	Limited

TABLE 2.5
MAC HF REQUIREMENTS

	<u>SYSTEM APPLICATION</u>	
	<u>GROUND-AIR-GROUND</u>	<u>GROUND-GROUND</u>
<u>INFORMATION TYPES</u>		
VOICE	Clear, Secure, AJ (1990)	Clear, Secure, AJ (1990)
TTY (<300 wpm)	Clear, Secure, AJ (1990)	Secure, AJ (1990)
DATA (>300 wpm)	Secure	Secure, AJ (1990)
<u>TRAFFIC PARAMETERS</u>		
MESSAGE LENGTH	10's words	100-5000 words
LOADING	170 Missions/day --- Peacetime >1000 Sorties/day --- Wartime	
TYPE	Point to Point	Primary
	Group	-----
	Broadcast	-----
TERMINAL TYPE/NUMBER	Airborne	-----
	Ground Fixed	See AFCS
	Ground Mobile	71 CCT;s* 27 ALCE; ALCC
<u>TIMELINESS</u>	<10 Minutes Connectivity	
<u>SECURITY</u>	Yes	Yes
<u>INTEROPERABILITY</u>		
INTRA AIR FORCE	HQ MAC, # Air Forces, TAF, SAC	
INTER SERVICE	Yes	Yes (Voice Only)
NATO	Yes	Yes (ALCC, ALCE, TALO, CCT)
CANADA	Yes	Yes (ALCC, ALCE, TALO, CCT)
*75 TALO, (TAC, PACAF, USAFE)		

TABLE 2.6

TAC HF REQUIREMENTS

	<u>SYSTEM APPLICATION</u>		
	<u>AIR REQUEST</u>	<u>FACP</u>	<u>TACC/E3A/NAVY</u>
<u>INFORMATION TYPES</u>			
VOICE	Secure, AJ	Secure, AJ	Secure, AJ
TTY (<300 wpm)	Burst, Preformatted	Secure, AJ	Secure, AJ
DATA (>300 wpm)	-----	Secure, AJ (TADIL A or J)	TADIL A or J
<u>TRAFFIC PARAMETERS</u>			
MESSAGE LENGTH	10's of words	short	short
LOADING	5 min/hr/terminal	continuous	continuous
TYPE			
Point to Point	Primary	Primary	Primary
Group	Moderate	Moderate	Moderate
Broadcast	None	None	None
TERMINAL TYPE/NUMBER			
Airborne	FAC	None	≈20
Ground Fixed	5	None	None
Ground Mobile	100's	Transport- ble ≈25	Transportable 5
<u>TIMELINESS</u>	Seconds	Seconds	Seconds
<u>SECURITY</u>	Yes	Yes	Yes
<u>INTEROPERABILITY</u>			
INTRA AIR FORCE	Yes	Yes	Yes
INTER SERVICE	Yes	Yes	Yes
NATO	Yes	No	Yes
CANADA	Yes	No	Yes

TABLE 2.7

AF COMM COM HF REQUIREMENTS

	<u>SYSTEM APPLICATION</u>		
	<u>SAC GROUND ENTRY</u>	<u>AERO STATIONS GROUND ENTRY</u>	<u>DCS</u>
<u>INFORMATION TYPES</u>			
VOICE	Secure, AJ	Clear, Secure AJ (1990)	Clear, Secure, AJ
TTY (<300 wpm)	Secure, AJ	Clear, Secure, AJ (1990)	Secure, AJ
DATA (>300 wpm)	-----	Secure	1200 bps
<u>TRAFFIC PARAMETERS</u>			
MESSAGE LENGTH	10-100's words	10's words	continuous
LOADING	4-12 channels	4-12 channels	4 channels
TYPE			
Point to Point		Primary	Primary
Group	All Apply	Moderate	None
Broadcast		Limited	None
TERMINAL TYPE/NUMBER			
Airborne	-----	-----	-----
Ground Fixed	9	18	15
Ground Mobile	-----	-----	29
<u>TIMELINESS</u>	20 Min. Authenti- cated Receipt	<10 Min Connectivity	Minutes
<u>SECURITY</u>	Yes	Yes	Yes
<u>INTEROPERABILITY</u>			
INTRA AIR FORCE	No	Yes	No
INTER SERVICE	No	Yes	Yes
NATO	Limited	Yes	No
CANADA	Limited	Yes	No

TABLE 2.8
AFLC HF REQUIREMENTS

<u>SYSTEM APPLICATION</u>	
<u>SRR AND DISASTER PREPAREDNESS</u>	
<u>INFORMATION TYPES</u>	
VOICE	Clear and Secure
TTY (<300 wpm)	Secure
DATA (>300 wpm)	Far Term (4800 bps) computer links
<u>TRAFFIC PARAMETERS</u>	
MESSAGE LENGTH	<500 Words
LOADING	One Channel
TYPE	
Point to Point	Primary
Group	Limited
Broadcast	Limited
TERMINAL TYPE/NUMBER	
Airborne	0
Ground Fixed	13
Ground Mobile	13
<u>TIMELINESS</u>	Minutes to Hours
<u>SECURITY</u>	Yes
<u>INTEROPERABILITY</u>	
INTRA AIR FORCE	Yes
INTER SERVICE	Yes
NATO	No
CANADA	No

TABLE 2.9
ADCOM HF REQUIREMENTS

	<u>SYSTEM APPLICATION</u>		
		<u>SENSOR SITES</u>	
<u>INFORMATION TYPES</u>	<u>E3A</u>	<u>CMD & CONTROL</u>	<u>WARNING DATA</u>
VOICE	Clear, Secure, AJ	Secure	Secure
TTY (<300 wpm)	-----	Secure	-----
DATA (>300 wpm)	TADIL-A ¹³⁶⁴ ₂₂₆₅ AJ & Secure	---	1200bps/2400bps AJ and Secure
<u>TRAFFIC PARAMETERS</u>			
MESSAGE LENGTH	---	10's of words	Continuous
LOADING	4-5 Channels	1 Channel/ Site	Continuous
TYPE			
Point to Point	Primary	Primary	Primary
Group	Moderate	Moderate	Moderate
Broadcast	None	None	None
TERMINAL TYPE/NUMBER			
Airborne	≈20	---	---
Ground Fixed	≈50	11	11
Ground Mobile	0	5	5
<u>TIMELINESS</u>	Seconds	Seconds	Seconds
<u>SECURITY</u>	Yes	Yes	Yes
<u>INTEROPERABILITY</u>			
INTRA AIR FORCE	Yes	Info	No
INTER SERVICE	Yes	Info	No
NATO	Info	Info	No
CANADA	Yes	Info	No

TABLE 2.10
ESC HF REQUIREMENTS

<u>INFORMATION TYPES</u>	<u>SYSTEM APPLICATION</u>	
	<u>GROUND-AIR-GROUND</u>	<u>GROUND-GROUND</u>
VOICE	Secure, AJ	Secure, AJ
TTY (<300 wpm)	Secure, AJ	Secure, AJ
DATA (>300 wpm)	-----	Secure, AJ
<u>TRAFFIC PARAMETERS</u>		
MESSAGE LENGTH	10's of words	100's of words
LOADING	Light	Moderate
TYPE		
Point to Point	Primary	Primary
Group	Limited	Limited
Broadcast	Limited	None
TERMINAL TYPE/NUMBER		
Airborne	≈20	0
Ground Fixed	See AFCS AERO Sta.	5
Ground Mobile	0	10's
<u>TIMELINESS</u>	Seconds	Minutes
<u>SECURITY</u>	Yes	Yes
<u>INTEROPERABILITY</u>		
INTRA AIR FORCE	Yes	Yes
INTER SERVICE	Yes	Yes
NATO	No	No
CANADA	No	No

TABLE 2.11
USAFE HF REQUIREMENTS

	<u>SYSTEM APPLICATION</u>	
	<u>USEUCOM CEMETERY NET</u>	<u>USAFE INFORM</u>
<u>INFORMATION TYPES</u>		
VOICE	Secure, AJ	Secure, AJ
TTY (<300 wpm)	Secure, AJ	-----
DATA (>300 wpm)	-----	-----
<u>TRAFFIC PARAMETERS</u>		
MESSAGE LENGTH	Max. 2000 characters	200 characters
LOADING	-----	Ea. ½ hr/3 min MSG
TYPE		
Point to Point		
Group	All Apply	All Apply
Broadcast		
TERMINAL TYPE/NUMBER		
Airborne	3 (WWABCP)	
Ground Fixed	7	75-100
Ground Mobile	180	
<u>TIMELINESS</u>	Minutes	Minutes
<u>SECURITY</u>	Yes	Yes
<u>INTEROPERABILITY</u>		
INTRA AIR FORCE	Yes	Yes
INTER SERVICE	Yes	Yes
NATO	Yes	Yes
CANADA	No	No

TABLE 2.12
PACAF HF REQUIREMENTS

	<u>SYSTEM APPLICATION</u>		
	<u>AIR REQUEST</u>	<u>EAM DISSEMINATION</u>	<u>E3A/NAVY</u>
<u>INFORMATION TYPES</u>			
VOICE	Secure, AJ	Secure, AJ	Secure, AJ
TTY (<300 wpm)	Burst, Preformatted	Secure, AJ	Secure, AJ
DATA (>300 wpm)	-----	-----	TADIL A
<u>TRAFFIC PARAMETERS</u>			
MESSAGE LENGTH	10's of words	200 characters	Short
LOADING	5 min/hr/terminal	-----	Continuous
TYPE			
Point to Point	Primary	Limited	Primary
Group	Moderate	Moderate	Moderate
Broadcast	None	Primary	None
<u>TERMINAL TYPE/NUMBER</u>			
Airborne	139		
Ground Fixed	215	(Represents Total Assets Needed)	
Ground Mobile	65		
<u>TIMELINESS</u>	Seconds	Seconds	Seconds
<u>SECURITY</u>	Yes	Yes	Yes
<u>INTEROPERABILITY</u>			
INTRA AIR FORCE	Yes	SAC	Yes
INTER SERVICE	Yes	Yes	Yes
KOREA	Yes	Limited	Yes
JAPAN	Yes	Limited	Yes
PHILIPPINES	Yes	Limited	Yes

"interoperability traffic", however, some insight into organizational interoperability can be gleaned from this data. For example, secure voice and data seem to be almost universally required with some sort of AJ protection usually desired also. Timeliness requirements are generally in the seconds to minutes area and messages are more often "short" than "long".

The conclusions reached for interservice traffic are as follows:

1. Data is used as much as voice. 51% of the messages use voice and 49% use data.
2. Most data messages are sent at low baud rates (i.e. 75 baud).
3. 73% of the messages are sent secure and 27% in the clear.
4. 55% of the missions require link timeliness in minutes.
5. 75% of the messages last for minutes and 14% are less than one minute.
6. Most (i.e., 57%) interservice networks use single-channel point-to-point communications in a half-duplex (44%) or simplex (34%) mode.

3.0 GATEWAY INTEROPERABILITY

The purpose of this section is to examine the issue of interoperability between dissimilar networks via a gateway. We shall do this by considering the feasibility of interfacing an HF communications network with the ARPANET. The issues raised during this investigation are generally applicable to generic gateways and hence this example will serve as a general discussion on gateway interoperability. Also considered is the possibility of such an interface with the Packet Radio Network (PRNET) currently being tested and developed by SRI International.

Work along lines similar to these HF/ARPANET/PRNET interfaces is being pursued in regard to the Defense Data Network (DDN) where problems associated with the interconnection of various computer networks are considered. Currently, SRI has an IR&D project in which an HF interface to PRNET is under study. PRNET has been successfully interfaced to ARPANET.

3.1 Characteristics of the ARPANET

This subsection contains a brief description of the components and capabilities of the ARPANET. The ARPANET protocols are discussed in Section 3.4.

The ARPANET is a packet-switched computer network originally conceived as a resource-sharing network among a group of computing centers funded and sponsored by the U.S. Defense Advanced Research Projects Agency (DARPA). It has become an object of continuing research into data communications and distributed data processing and continues to grow in size and capabilities.

The network switches in the ARPANET are known as Interface Message Processors (IMP), and are tied together with 50 kb/s telephone lines. An IMP is tied directly to a computer (called a Host) through an interface designed by Bolt, Beranek, and Newman (BBN) of Cambridge, Massachusetts. Injection of a message into the ARPANET through an IMP must be accomplished via the Host.

A user wishing to access the ARPANET without going through a Host can use a terminal connected to a Terminal Access Controller (TAC). The TAC is a BBN C-30 minicomputer that supports up to sixty-three asynchronous terminal ports. Currently, subscribers can connect terminals and modems that conform to the RS-232-C interface specification to a TAC. The TAC supports communications at data rates from 75 to 9600 b/s. There is also another device for direct terminal injection into the ARPANET known as a mini-TAC. The mini-TAC has up to sixteen terminal ports and operates at 110 to 19200 b/s.

Host computers communicate with each other using messages that are about 8,000 bits long. These messages are divided into packets of about 1,000 bits by the switches and sent over the communications subnet. Maximum end-to-end delays are a few hundred milliseconds and host-to-host throughputs are measured in tens of thousands of bits/second.

When all the packets associated with a particular message arrive at the destination switch, they are reassembled to form the original message, which is passed to the destination host. The destination switch then returns a positive acknowledgement (ACK) to the source host.

Rather than simply confirming delivery, the message acknowledgement assumes that a subsequent message will follow immediately on the same connection. Therefore, the delivery acknowledgement is known as a RFNM (Request For Next Message). If a message cannot be delivered owing to a line failure, a node failure, or missing packets, an incomplete message will be returned, thus initiating a retransmission. If neither a RFNM nor an incomplete message arrives back at the source during a suitable timeout interval, the message will be reinitiated.

The new message flow generates the entry of information into a "Pending Leader Table" (PLT), which the originating switch uses to create the packet headers for the individual packets of the message from the user-supplied packet leader information. At the same time, the originating switch requests the destination switch to allocate a set of buffers for the reassembly of the individual packets into the complete message segment for delivery to the destination host. The allocation request (REQALL) transits the network rapidly as a short control/information packet. If the required buffers are available at the destination switch, the destination switch returns an allocation (ALL) control message to the originating switch, which can then commence transmission of the individual packets composing the message.

Despite the fact that the packets are transmitted in sequence by the originating switch, the network operation, employing error correction, dynamic routing, and other features that affect the end-to-end delay, may cause the packets to arrive at the destination switch in a different sequence. When the message is fully reassembled in the destination switch buffers, it can then be

relayed to the destination host. The destination switch then transmits an acknowledgement in the form of the RFNM, together with an allocation for additional message segments. If for some reason no buffers are available after delivery of the current message segment, it is possible to return the RFNM without an allocation.

While all of this is occurring on an end-to-end basis, each packet transmitted within the network is acknowledged on a link, switch-to-switch basis, to insure proper delivery and error-free transmission. The control packets, such as the REQALL and RFNMs, flow through the network in much the same way as the user data packets do.

The basic mode of operation in the ARPANET, in conjunction with the required host-to-switch protocol functions, is known as virtual circuit. Virtual circuit can be defined by the properties it must have. These properties include sequenced data transfer, data transparency, a full-duplex path, in-band and out-of-band signaling, flow control, error control, interface independence, and a switchable form of operation. The following is a brief description of the properties of virtual circuit:

Sequenced Data Transfer

All data bits delivered to the destination host must be in the same order they were delivered to the network by the source host. This property implies the need for the message reassembly process.

Data Transparency

Data bits in the user data fields must be accepted in any sequence of ones and zeros. No sequence may be prohibited, despite the fact that special bit groups are needed to "flag" the beginning and end of packets. This property implies the need for special handling of the data stream to protect against inadvertent flag sequences.

Full-Duplex Path

Data has to be able to flow in both directions between the end users simultaneously. Thus, the initiation of a connection and buffering for a message in one direction requires a similar process in the opposite direction.

In-Band/Out-of-Band Signaling

Signals have to move between the users and the switches in order to control the flow of information, to inform the user of status information, to respond to network or user inquiries, etc. This signaling can take place as part of the normal user data stream (in-band) or outside the normal user data transmissions (out-of-band).

Flow Control

The network must be capable of reducing the allowed input rate of information. This is important to prevent congestion to the point where normal operation may become impossible.

Error Control

All network transmission must be error protected, so that the probability of an undetected network-introduced error will be negligible.

Interface Independence

Operation of the network must be independent of the physical and electrical properties of the user interface. It must be consistent with the logical data structures.

Switchability

Network operation in the virtual circuit mode allows information to be exchanged among various user pairs by modifying the address field of the user segments.

Further details on the operation of the ARPANET can be found in Section 3.4.

3.2 Characteristics of a PRNET

The following is a brief description of a PRNET as it currently exists. Additional features, which will be available in the near future, are also discussed.

A PRNET is a packet-switched, broadcast network of any combination of fixed, ground-mobile, or air-mobile nodes. Each node has a Packet Radio Unit (PRU) consisting of an L-band spread-spectrum radio unit, an omnidirectional antenna, and a digital unit. The radio characteristics are shown in Table 3.1. This particular version of a packet radio is known as an Experimental Packet Radio (EPR).

Table 3.1 lists two data rates for the radio. Normally, the radio operates at 400 kbps unless the noise and/or multipath environment becomes too severe, then a 100 kbps rate is automatically invoked.

The packet radio receiver uses post-detection integration that extends over one-third of a bit time. This feature gains some degree of multipath resistance at the expense of some spread-spectrum time-capture potential.

An updated version of the packet radio is currently under development. This new version, the Low-Cost Packet Radio (LPR), will be smaller in size and will support pseudo-noise code, changing for every bit.

TABLE 3.1

EXPERIMENTAL PACKET RADIO CHARACTERISTICS

Frequency band	1710 to 1850 MHz
Tuning	Digitally controlled synthesizer
Occupied bandwidth	20 MHz (for 99.5% of radiated energy)
Maximum output power	10 W
Spread-spectrum technique	Direct sequence PN code
Receiver threshold level	-99 dBm to -20 dBm (100 kbps) -93 dBm to -20 dBm (400 kbps)
Data rate (dual)	100 (400) kbps
Data modulation	DPSK
Chip modulation	MS, (minimum shift keyed)
Bit modulation	Differentially coherent
Spread factor	128 (32)
Processing gain	+21 dB (+15 dB)
PN decoding	Surface acoustic wave matched filter

A PRNET node can be one of three types. A node whose PRU is operated in "stand-alone" configuration is a repeater. If a subscriber is connected to a PRU through a Terminal Interface Unit (TIU) then the node is a terminal node. Each terminal node is capable of handling multiple users with the TIU functioning as a multiplexer. The TIU also contains the software for end-to-end protocols, traffic sources, and traffic measurements. The addition of a specially programmed PDP-11/23 microcomputer to a PRU makes the node a packet radio station. The station software contains the processes for network routing, diagnostics and traffic measurements. A station is normally also a terminal node.

Network management is accomplished by the station through the use of intranet packets exchanged between all network elements. Protocols exist that allow multiple stations to share the control of a particular network. A stationless protocol for reduced capacity operations is in the process of development. Network management tasks include initialization (including the addition or deletion of nodes), routing, access control, and flow control.

Packets are transported through the network on a store-and-forward basis using buffers within each PRU and a hop transport protocol between them. Packets for forwarding are broadcast from a node (PRU), but are selectively addressed to a single PR identified in the packet header. The relay process proceeds until the destination PRU is reached, at which time the packet is passed across an interface to an attached subscriber device (e.g., a video terminal). Positive acknowledgments (ACK) are required on a

hop-by-hop (HBH) basis along the route. Each time an acknowledgment is not received for a packet (for any reason), the PRU retransmits the packet. This process continues for a set number of retransmissions. Should this fail, a similar number of attempts are made to route the packet through alternative PRUs. If this fails, a new route is requested from the station and the packet is discarded to guard against deadlocks. Thus, the PRNET is potentially lossy.

Because retransmissions can lead to duplicate packets, duplicate filtering is also performed in each PRU.

In the current networks (composed of experimental packet radios), all users access the radio channel on the same frequency with the same spread-spectrum PN code. Access to the channel is controlled through protocols (called carrier-sense multiple access) to minimize packet "collisions". Allocation of system capacity to a user is based on dynamic demands made by the user (his packet offer rate).

Radios which would have individualized PN codes (and therefore eliminate contention problems) are in the process of development and are expected to be available early in 1987.

3.3 Protocols and Interfaces - General Concepts

Protocols and interfaces are distinguished as follows: protocols are procedures used by entities at the same "level" to communicate with one another; interfaces are procedures to enable entities at different levels to exchange information. The concept of a protocol level (or layer) will be explained below.

The general idea behind "layering" of protocols is to enable network entities of similar type to communicate with each other without concerning themselves with the problems associated with communication among network entities at other levels. For example, an entity at the "network layer" (refer to Figure 3.1) would use network level protocols to communicate with another network level entity. The actual flow of network level communication (system A to system B) would be to the data link level through an interface and then down another interface to the physical level. The information would then proceed through the physical interconnection media to system B and then up through system B's physical and data link layer to the recipient network level entity in system B. The network level entities (as well as the data link and physical level entities) would perceive this process as though they were in direct communication with each other.

The Reference Model of Open Systems Interconnection developed by the International Organization for Standardization (ISO) provides a generally accepted common reference for these relationships. This model defines seven protocol layers (or levels) of which four directly concern data exchange protocols used in data communication systems and three relate to management protocols used in the system.

The ISO model is shown in Figure 3.1. The functions of each level can be briefly described as follows:

Level 1 (Physical). Physical, electrical, and functional procedures used to establish, maintain, and disconnect

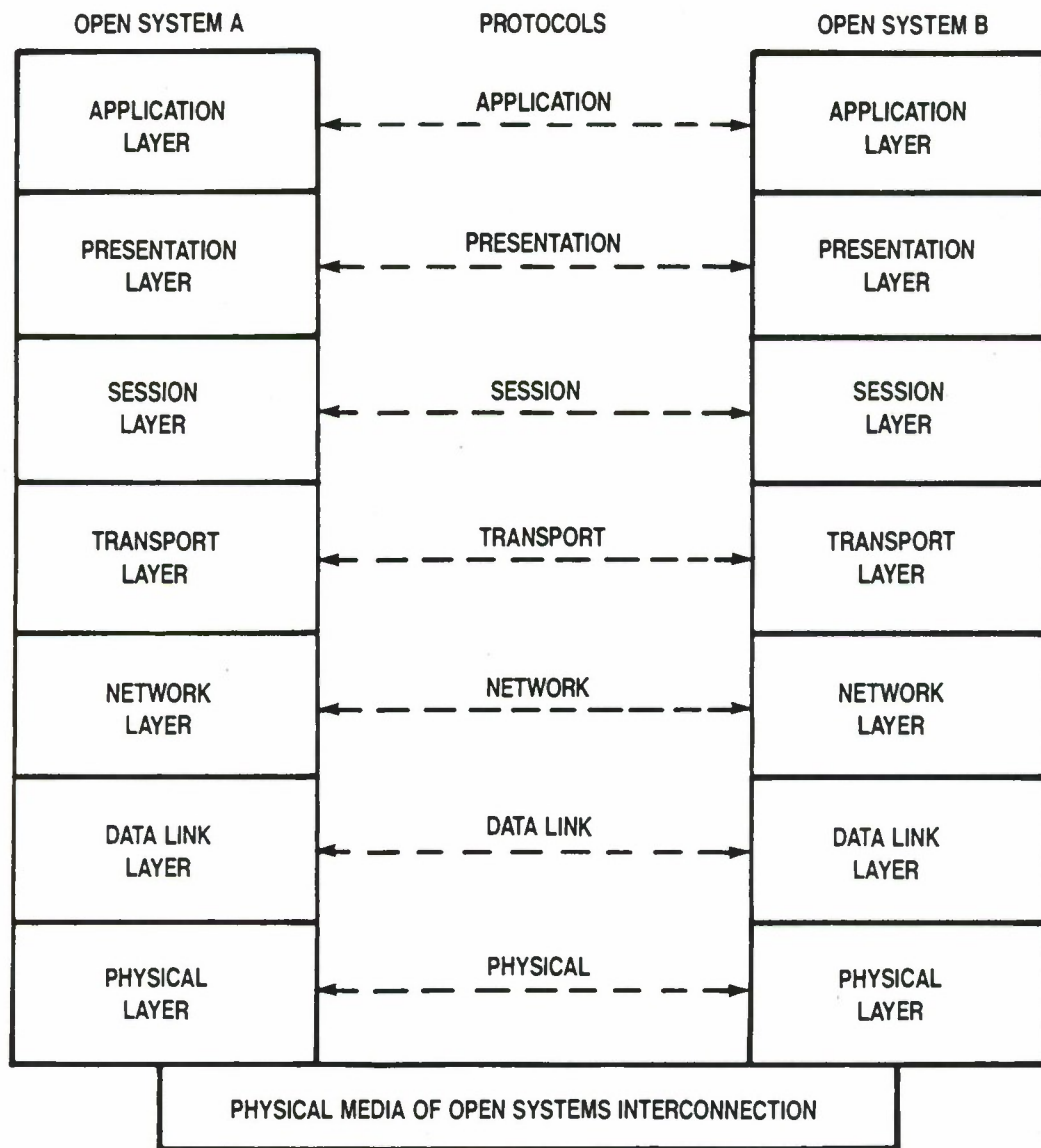


Figure 3.1. ISO Interface Model for Open Systems

the physical link between a data terminal equipment (DTE) and a data channel. Generally accepted standards, such as EIA RS-232-C, are currently being applied at this level.

Level 2 (Data Link). Functional procedures used to transfer error-free data between nodes in the network. The principal functions performed are link initialization, error control, flow control, and link assurance. Protocols with acronyms such as HDLC, ADCCP, SDLC, and LAP represent procedures currently used at this level.

Level 3 (Network). Functional procedures used to transfer data through the network nodes. Messages to be transported through the network are formatted and asynchronously time division multiplexed onto the data link channel provided by the Level 2 protocol. Message flow and error control are provided by this protocol layer. This level is also known as the packet layer.

Level 4 (Transport). This level provides the procedural interface between session entities. A session entity could be an application program, a user terminal, a sensor, etc. The communication system design is not directly affected by the protocol at this level.

Level 5 (Session). This protocol covers the cooperative relationship between presentation entities to facilitate communication, (i.e., terminal to data base).

Levels 6 (Presentation) and 7 (Application). Primarily management and monitor functions are exercised at these levels. Level 6 is concerned with format management to facilitate the interpretation of data being exchanged, while Level 7 is concerned with the management of interprocess communications.

3.4 ARPANET Protocols

The ARPANET protocols and interfaces are depicted in Figures 3.2 and 3.3.

The host software, which accomplishes host-to-host protocol functions, is a set of modules collectively known as the Network Control Program (NCP). The NCP in one host sets up a logical circuit called a "connection" with a NCP in another host and by means of this connection, enables distant processes to communicate with one another. The NCP receives data from a user process and formats it into an ARPANET-type message. This message is preceded by information used by the packet switching subnetwork and the destination host for routing and control purposes. Upon receipt by the destination host, NCP reformats the ARPANET-formatted message and passes it on to the correct user process. Essentially, the NCP is at the level of operating systems software.

The hardware and software interfaces for the connection between the host and IMP are specified in BBN Report No. 1822, "Specifications for the Interconnection of a Host and an IMP". To the host computer, the IMP appears to be another input/output

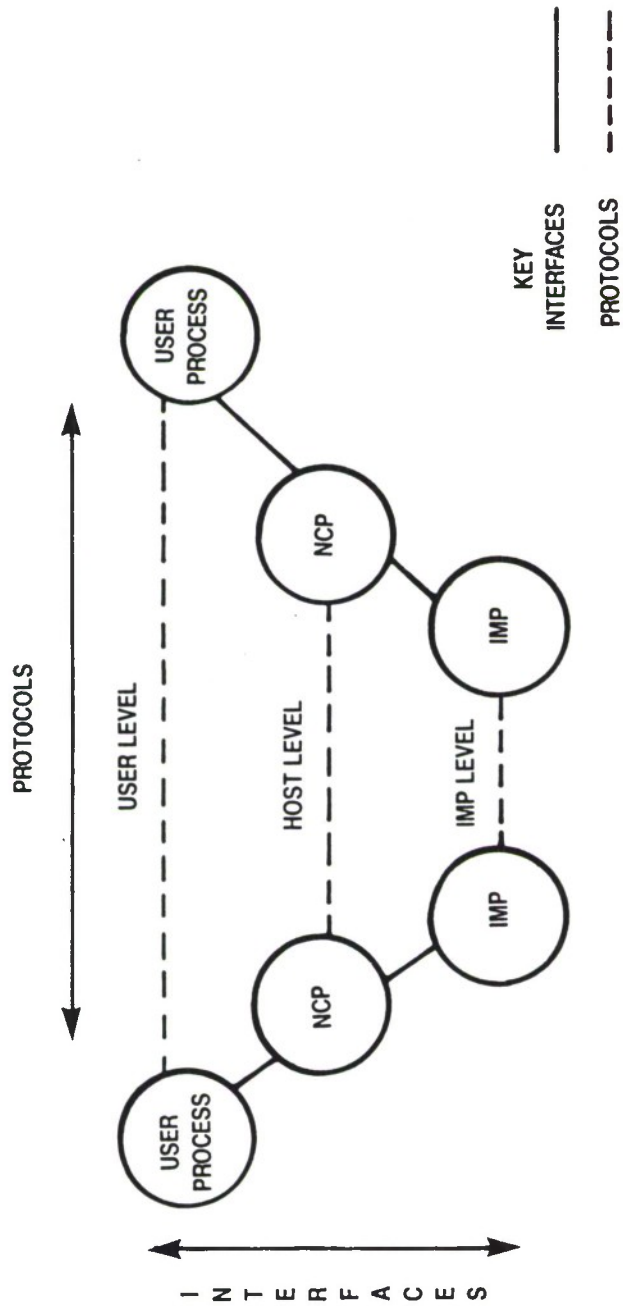


Figure 3.2. ARPANET Protocols and Interfaces

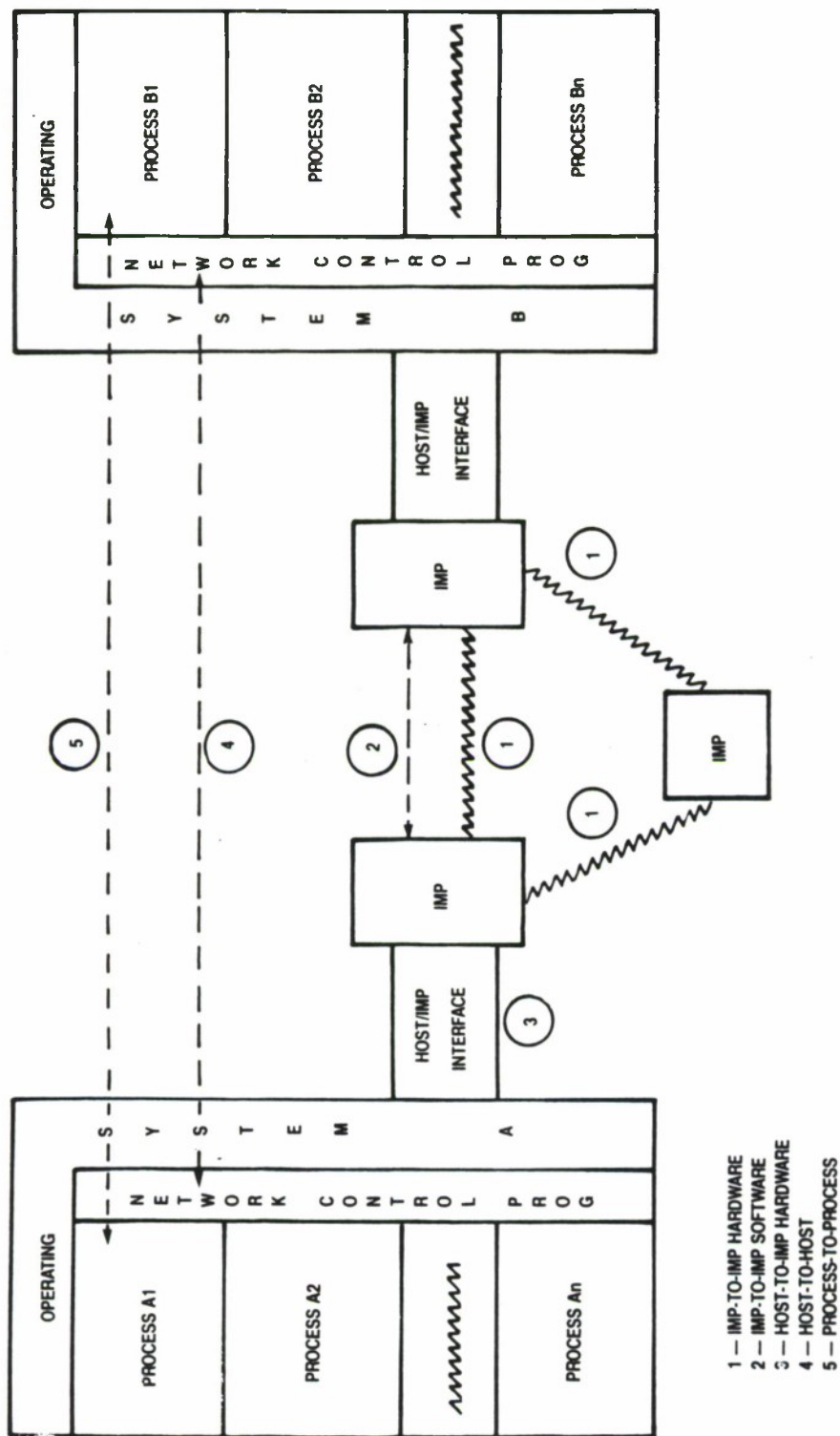


Figure 3.3. Further Details on ARPANET Protocols and Interfaces

device. A device specific module must be programmed to perform the mechanics of the data transfer between the two. This is one operating systems-level function which NCP performs.

NCP has built-in error control mechanisms which detect errors and perform remedial actions. On occasion, NCP aborts a connection upon detection of an error. NCP also uses special NCP-to-NCP control messages to deal with error situations. When an error is detected, time and circumstances are recorded. When the particular error warrants, the host computer operator is informed by NCP.

NCP uses buffers to assist in flow control. Due to the irregular flow rates through the packet switching subnetwork and the different speeds of process execution of sending and receiving hosts, these buffers are required. Also, NCP uses special "allocate" messages to reserve and manage buffer space in distant hosts. The allocate mechanism guarantees sufficient buffer space in the receiving host to accept a specific number of messages.

NCP also performs a multiplexing function. At any specific time no more than one message can be outstanding between hosts on a virtual connection. If a sending NCP transmits a message to a distant NCP, the IMP at the destination host must send back a special RFNM (Request for Next Message) control message acknowledging receipt and requesting another message. However, multiple processes in sending and receiving hosts may be transmitting to one another over many connections without knowing that their messages are being multiplexed in a single pipeline by NCP. Thus, many virtual circuits between conversing processes are achieved.

At the process level, users communicate by an agreed-upon set of procedures which is the user-level protocol. At the host level, NCPs communicate with one another by their host-to-host protocol. At the IMP level, IMPs communicate with another level of protocol. The IMP-to-IMP protocol is accomplished by special hardware and software in the IMPs.

The user process interfaces with NCP through a number of system calls such as OPEN, CLOSE, SEND, and RECEIVE. The user process is informed of the current status by an updated connection table accessible by the user process. The NCP interfaces with the IMP by means of a hardware coupler and special software commands, both of which are specified in BBN Report No. 1822.

The ARPANET protocol structure does not correspond exactly to that of Figure 3.1. Figure 3.2 is related to Figure 3.3 in that the user level of Figure 3.2 is equivalent to the session level of Figure 3.1. The HOST level is equivalent to the transport level and the IMP level is spread among the data link and physical levels. The physical media of the ARPANET is high speed (50 kbps) phone lines.

3.4.1 The TELNET Protocol

The purpose of the TELNET Protocol is to provide a general, bi-directional, eight-bit byte oriented communications facility. Its primary goal is to allow a standard method of interfacing

terminal devices and terminal-oriented processes to each other. It is envisioned that the protocol may also be used for terminal-to-terminal communication ("linking") and process-to-process communication (distributed computation).

TELNET is a presentation level protocol. A TELNET connection consists of a pair of standard Host/Host Protocol connections over which passes data with interspersed TELNET control information. The pair of connections are typically established by the Initial Connection Protocol.

The TELNET Protocol is built upon three main ideas: first, the concept of a "Network Virtual Terminal"; second, the principle of negotiated options; and third, a symmetric view of terminals and processes.

1. When a TELNET connection is first established, each end is assumed to originate and terminate at a "Network Virtual Terminal," or NVT. An NVT is an imaginary device which provides a standard, network-wide, intermediate representation of a canonical terminal. This eliminates the need for "server" and "user" Hosts* to keep information concerning the characteristics of each other's terminals and terminal handling conventions. All Hosts, both user and server, map

*Note: The "user" Host is the Host to which the physical terminal is normally attached, and the "server" Host is the Host which is normally providing some service. As an alternate point of view, applicable even in terminal-to-terminal or process-to-process communications, the "user" Host is the Host which initiated the communication.

their local device characteristics and conventions so as to appear to be dealing with an NVT over the network, and each can assume a similar mapping by the other party. The NVT is intended to strike a balance between being overly restricted (not providing Hosts a rich enough vocabulary for mapping into their local character sets), and being overly inclusive (penalizing users with modest terminals.)

2. The principle of negotiated options recognizes the fact that many sites will wish to provide additional services over and above those available within an NVT, and many users will have sophisticated terminals and would like to have elegant, rather than minimal services. Independent of, but structured within, the TELNET Protocol various "options" will be sanctioned which can be used with the "DO, DON'T, WILL, WON'T" structure (discussed below) to allow a user and server to agree to use a more elaborate (or perhaps just different) set of conventions for their TELNET connection. Such options could include changing the character set, the echo mode, the line width, the page length, etc.

The basic strategy for setting up the use of options is to have either party (or both) initiate a request that some option take effect. The other party may then

either accept or reject the request. If the request is accepted, the option immediately takes effect; if it is rejected, the associated aspect of the connection remains as specified for a NVT. Clearly, a party may always refuse a request to enable, and must never refuse a request to disable some option, since all parties must be prepared to support the NVT.

The syntax of option negotiation has been set up so that if both parties request an option simultaneously, each will see the other's request as the positive acknowledgment of its own.

3. The symmetry of the negotiation syntax can potentially lead to non-terminating acknowledgment loops, each party seeing the incoming commands not as acknowledgments but as new requests which must be acknowledged. To prevent such loops, the following rules prevail:
 - a. Parties may only request a change in option status; i.e., a party may not send out a "request" merely to announce what mode it is in.
 - b. If a party receives what appears to be a request to enter some mode it is already in, the request should not be acknowledged.
 - c. Whenever one party sends an option command to a second party, whether as a request or an acknowledg-

ment, and use of the option will have an effect on the processing of the data being sent from the first party to the second, then the command must be inserted in the data stream at the point where it is desired that it take effect. (It should be noted that some time will elapse between the transmission of a request and the receipt of an acknowledgment, which may be negative. Thus, a site may wish to buffer data after requesting an option, until it learns whether the request is accepted or rejected, in order to hide the "uncertainty period" from the user.)

3.4.2 The Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is intended to be used as a host-to-host protocol between hosts in a computer network or (more especially) between hosts in interconnected computer networks. TCP is, then, an internetwork host level protocol.

TCP is being used in the DARPA-sponsored work on PRNET and packet-switched satellite communication (SATNET), and interconnections of these experimental facilities with each other and the ARPANET. TCP implementations exist for PDP-10 TENEX systems, PDP-11 systems and other systems.

TCP is designed to support interprocess communication by establishing full-duplex logical connections between process input/output ports. The data exchanged between processes is a stream of octets divided into variable length letters. The TCP provides for reliable communication by using end-to-end

acknowledgments and checksums. TCP modules exchange control information to establish and terminate connections, to regulate the flow of data on connections, and to signal the need for urgent handling of a connection. The control information is communicated between TCP modules in the headers of messages on the data connections. There is no separate control connection. An Internetworking Protocol (IP) is used in conjunction with TCP.

3.5 Interconnecting Networks via Gateways

The interconnection of an HF network to PRNET or the ARPANET would be accomplished by means of a gateway. We shall refer to this gateway as a Black Box (BB) and shall consider what characteristics it should possess. It is desirable to design the BB in such a way so as to not affect the internal operations of the individual networks. A BB could be made to appear to the network as either a terminal or a Host.

Gateways are hardware and software interface and translation services that allow two or more local networks to be interconnected. They are either separate, well defined hardware/software nodes, part of host computers, or other devices. Gateways may perform electrical, protocol, character, or user-to-user translations, complex routing, or initiate communication onto one of the attached networks. The following list of characteristics are generally ascribed to gateways:

1. Message passing capability between connected local networks,
2. Access control mechanisms,

3. Segmentation/collection capabilities,
4. Congestion and flow control capabilities,
5. Accounting mechanisms, and
6. Inter-gateway retransmission capability.

One disadvantage of the gateway approach may be protocol incompatibility, because of possible difficulties in finding matching equivalent sets of services at all levels of the standard OSI protocol model. Interconnection of local networks may become more complicated if the individual networks operate at different speeds or if they have different levels of security.

3.5.1 Interconnect Level

Network interconnections may be made at either the application level or device level. Connection at the application level assumes that the gateways have knowledge of the application protocol layer and can translate requests on one network into requests of a similar application protocol on another network. In general, translating one application protocol into another results in retention of only the functionality common to both. Requests that must cross several networks and which are translated several times along the way, will probably suffer a loss of functionality and a loss in efficiency.

Interconnection of networks at the host or device level reduces the complexity of the gateways by limiting their tasks to

transmission of internetwork packets and associated tasks, such as routing and connection management. Interconnection at this host level requires that higher level protocols for different networks be the same, but does not necessarily require that a current set of higher level protocols on each network be replaced. An internetwork protocol is used to provide a uniform framework for communication over these different interconnected networks. For HF injection into the ARPANET or PRNET, it would require the use of the ARPANET TCP/IP protocols.

3.5.2 Type of Service

Either a datagram (connectionless) or a virtual circuit (connection-oriented) type of service may be used in interconnecting local networks. With the datagram service, each datagram or packet contains enough information to allow independent routing and delivery of the message. The virtual circuit service allows the establishment of logical connections at the internetwork level between source and destination hosts or devices on different networks.

A datagram service at the internetwork level is simpler and less expensive than a virtual circuit service. The protocols are less complicated, status information does not have to be sorted, and a minimum amount of message handling is required. Virtual circuit service provides a highly reliable sequence service. It is especially useful if the interconnected networks are similar. The ARPANET is a virtual circuit network although TCP/IP present messages to the network as datagrams.

3.5.3 Addressing

Either a flat or a hierarchical addressing scheme can be used with interconnected local networks. With a flat addressing scheme, individual devices can be permanently assigned a network address. The gateways would have to store addressing information in order to locate a particular destination.

In a hierarchical addressing scheme, the first part of the address designates an individual network and the remainder identifies particular addresses within each network. These addresses within a local network are based on that local network's addressing scheme. With hierarchical addressing, gateways only have to examine the network part of the address. Hierarchical addressing techniques allow for greater flexibility in the interconnection of networks, especially future interconnections.

If we are dealing with an HF/ARPANET connection, where the ARPANET is not to be used as a transit net, then flat addressing is sufficient. If the connection is HF to PRNET to ARPANET, or if the ARPANET is to be used as a transit net, the hierarchical addressing scheme should be considered.

3.5.4 Routing

Internetwork routing is important when there are multiple gateways or paths from one local network to another. Multiple gateways may be used to improve overall reliability efficiency. Gateways may maintain information about their connectivity to all networks and to all gateways. Then, with a dynamic routing scheme, the required level of service in the network can be maintained in the face of such temporary network conditions as congestion or

failed links. Either fixed or dynamic routing schemes involving gateways can be developed as a function of security levels, packet size, traffic load, priority, and other factors.

3.5.5 Segmentation/Collection

The different local networks used in an interconnected system will have a range of maximum packet or message sizes. In going from a network that supports only small packets to one that supports large packets, a greater degree of efficiency may be obtained by combining the packets at the gateway for transmission onto the large packet network. In going from networks that support large packets to those that can only support a smaller sized packet, the large packets can be divided into multiple packets at the gateway. Each of these smaller packets will then have its own internetwork header and trailer for delivery across that particular network.

3.5.6 Flow Control

In a system with different local networks operating at different speeds, some form of flow control mechanism is needed to control the rate of transmission of information onto the slower-speed network. Flow control techniques that may be used include transmission only when exclusively permitted, forcing source hosts or devices to reduce their offered load, and an advisory type of service that informs the source that messages may be discarded because of congestion or other problems. All of these techniques serve to limit the rate at which the connected network receives information. HF networks operate at data rates considerably less than that of the ARPANET or PRNET.

3.5.7 Reliability

The reliability of interconnected local networks is no better than the reliability of the individual networks. Usually reliability can be improved only by adding considerable complexity to the gateways. Gateways can be used to guarantee that packets do not loop indefinitely among gateways, to trace the route that a message follows from source to destination, to send error reports to sources or other gateways, and to provide retransmission across a particular network.

3.5.8 Security

Interconnecting local networks may present a security problem. Messages from a secure local network to another secure local network should not be routed through a non-secured, intermediate network or one that has a lower level of security. Gateways may be able to detect the security level and stop transmission, but this, in itself, may offer a point of vulnerability in the secure network. Security issues are considered further in Section 5.

3.5.9 Broadcast Support

Many local networks have a broadcast feature that allows a single message from a source to be sent to all of the stations on a network or to some preselected subgroup. These types of broadcast transmissions require that every station on the network or every station in the subgroup handle the particular message. Because of this, it is not clear if a broadcast capability should be included

in an interconnected system of local networks. Since the ARPANET is not a broadcast network, the HF/ARPANET gateway must block the injection of HF network broadcast messages into the ARPANET. PRNET delivers messages by a broadcast technique but the messages themselves are point-to-point.

3.5.10 Gateway Hardware Characteristics

The PRNET TIU is accessed by a RS-232-C interface link. ARPANET TACs and Hosts also support this interface. RS-232-C is described in detail in Appendix A. Other possibilities for the physical interface are, RS-449, FED-STD-1031, MIL-STD-188C, and MIL-STD-188-114.

3.5.11 BB Connection to a Host - BB Appears as a Terminal

Either full service or limited service interfaces are available for a BB/Host connection.

The full service connection provides full ARPANET functionality and supports all ARPANET protocols. Any interface which does not support the above is deemed a limited service interface.

Full service interfaces would use the ARPANET access protocols and would require the use of its ARPANET application level protocols as well as TCP/IP.

Network protocols may be integrated into a full service system in either an inboard (in the host computer) or an outboard (in a communications processor attached to the host computer) implementation.

In inboard implementations, the network protocols can be written as user-level applications or as operating system functions. The user-level approach has the advantage of simplicity; the protocols can be implemented in a familiar, well-structured programming environment. However, the execution environment provided by operating systems to user processes is, in general, not well suited to the requirements of network protocols. Therefore, user-level implementations may result in poor performance. Conversely, the operating system approach offers a less favorable programming environment but a more favorable execution environment. Unfortunately, some of the requirements of network protocols are not met by the services and capabilities available to operating system processes. Attempting to meet those requirements while still preserving the integrity of the operating system can be a formidable task.

The other alternative is an outboard implementation, where the network protocols are moved to a separate front-end-processor. This approach provides a dedicated environment that can be tailored to the specific needs of the network protocols. The outboard approach is not completely free of problems, however. The cost of a separate box may be incurred. Also, a communication mechanism must be provided between the host system and the front-end processor. Although it is subject to the same processing considerations as the inboard implementation, this mechanism, commonly referred to as a host-to-front-end protocol, is normally easier to implement. In addition to the host-to-front-end protocol implementation in the host, the application protocols must also be implemented.

An example of a limited service interface is the Terminal Emulation Processor (TEP). A standard TEP will support sixteen terminal connections to the Host. The TEP implements TCP/IP and provides a standard ARPANET connection to the network. In addition, the TEP implements the "server" or Host portion of the TELNET protocol. In its configuration, the TEP will only support asynchronous connections to the Host. With the addition of synchronous interface support, the TEP may be used to provide remote synchronous terminal-to-host communication.

3.5.12 BB Connection to a TAC - BB Appears as a Terminal

Direct connection of terminals (or the BB) to the network can be supported by two devices. The devices are the Terminal Access Controller (TAC) and a smaller version known as the mini-TAC.

The TAC allows a terminal user to communicate with any Host on the network without going through an intervening local Host. All terminal-to-host connections are multiplexed over a single link between the TAC and the switching node.

A TAC port supports only asynchronous operation.

Subscribers have indicated that a low-cost means of terminal access is required in locations with fewer terminals than are currently supported by the TAC. In these situations, a microprocessor-based device known as the mini-TAC can be provided to support up to 16 terminal connections to the network. The mini-TAC is a standard configuration of the Defense Data Network (DDN) Network

Access Component. Both the TAC and the mini-TAC implement TCP/IP and provide a standard ARPANET connection to the network. In addition, the TAC and the mini-TAC implement the "user" portion of the TELNET protocol.

The mini-TAC will support both asynchronous and synchronous terminals. The types of vendor-unique synchronous terminals to be supported will be based on subscriber requirements and priorities. The protocols implemented in a particular mini-TAC will be those necessary to support the terminals attached to it. Terminals connected in asynchronous mode will be able to communicate at data rates from 110 to 19,200 bits per second and in synchronous mode from 1,200 to 19,200 bits per second.

3.5.13 BB Appears as a Host

If the BB were to be configured to appear to the network as a Host, then the full set of Host-to-Host and higher level protocols would have to be implemented. Also a Host port would have to be obtained.

The Host to IMP interface is an 1822 interface rather than an RS-232-C and the 1822 protocols would have to be implemented.

3.6 Conclusions Regarding an HF/ARPANET/PRNET Interface

The construction of a HF interface to the ARPANET and/or PRNET should certainly be feasible. Probably the only reason one does not now exist is that there has been no reason to have one. Computer networks (like ARPANET) do not normally run at HF frequencies, as the data rates that HF will support are generally too low. PRNET

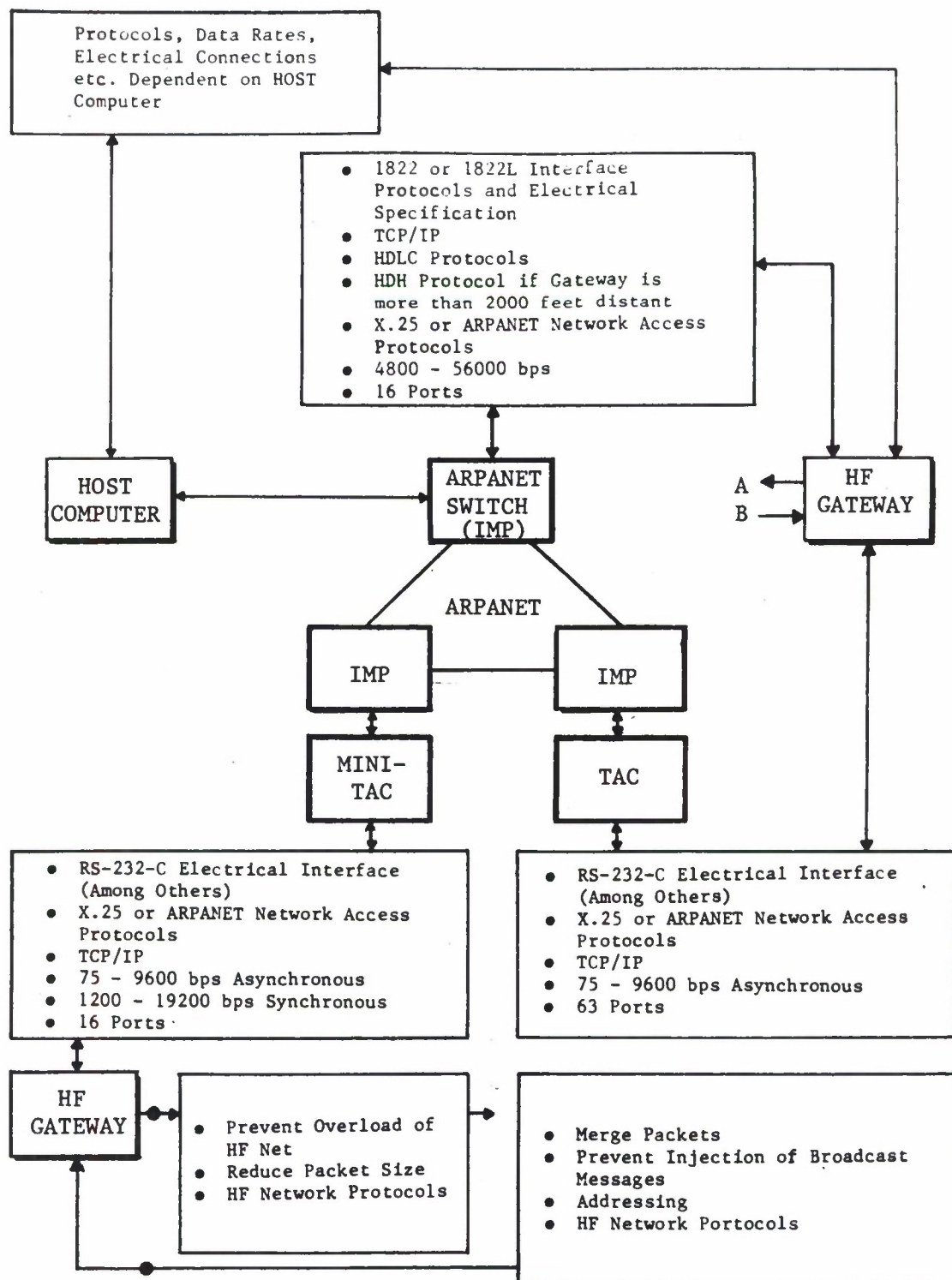


Figure 3.4. HF/ARPANET Interface Considerations

has been tested and developed primarily for tactical use and has, therefore, not required long range (i.e., HF) communication. PRNET, quite naturally, would therefore use frequencies (like UHF) where the wavelengths were "short enough" to avoid the physical problems (large antennas, etc.) associated with HF communication.

3.6.1 HF Interface to PRNET

An HF interface to PRNET would be accomplished by connecting a gateway to a PRNET TIU. This connection can be an RS-232-C or alternatively an RS-449, FED STD-1031, MIL-STD-188C or MIL-STD-188-114. Protocol, data rate, flow control, addressing, and security considerations are the same as for the ARPANET and are covered below.

3.6.2 HF Interface to the ARPANET

An HF network could be connected to the ARPANET in several ways. In general, Command Centers and other important entities would probably have access to an ARPANET (or DDN) Host computer either directly or through some dedicated asset. The question of access by the force elements is a different matter. This would involve the creation of an HF gateway to the ARPANET which would allow remote access of the gateway to be accomplished in a simple and efficient manner. Figure 3.4 depicts the possible configurations of such a connection and highlights the important issues. Basically the HF gateway could appear to the network as a Host computer (i.e., connected directly to an IMP) or as a terminal. If the gateway is to appear as a terminal, then it can be connected either directly to a Host computer or through a TAC or mini-TAC.

If the gateway were to be connected directly to an IMP then, since HF traffic is low in terms of bits per second and in number of messages, an inefficient utilization of a valuable IMP port would result. Also, the protocols and electrical connections are more complicated than if the gateway were to be connected to a TAC or mini-TAC.

If the gateway were to be connected directly to a Host computer, then the number of different versions of gateways required would depend on the various types of Host computers (there are a number of them). In the interest of standardization it seems wiser to attach the gateway to a TAC or mini-TAC.

3.6.3 HF Gateway Characteristics

The HF gateway can be viewed as a two-sided device with one side in the ARPANET via a TAC or mini-TAC and the other side in the HF net. The ARPANET side of the gateway should have the following characteristics.

1. The physical interface should be an RS-232-C or similar type.
2. TCP/IP are needed. IP has eight levels of message precedence that need to be specified.
3. Either X.25 or the ARPANET access protocols should be used.
4. There are 16 ports into a mini-TAC and 63 ports into a TAC. If the HF traffic is not anticipated to be great enough to

require an entire port, the port can be shared by a statistical multiplexer. Statistical multiplexers have been developed for both TACs and mini-TACs.

5. Both the TAC and the mini-TAC run at 75-9600 bps, asynchronously. The TAC cannot run synchronously. The mini-TAC runs at 1200-19200 bps in the synchronous mode. Since HF data rates are generally quite low, the ability to use both TAC and mini-TAC ports would seem to offset the higher data rates achievable by synchronous operation and argue in favor of asynchronous operation for the ARPANET side of the HF gateway.

The HF network side of the gateway should possess the following characteristics.

1. Packet size must be adjusted. The ARPANET will return packets of up to 1000 bits in length and messages of up to 8000 bits. This is too long for HF networks that do not possess sophisticated error control techniques. Also, the packets from the HF network to the ARPANET are likely to be quite short and in order to efficiently utilize the ARPANET it is probably wise to combine several short packets into longer ones whenever feasible.
2. Since the capacity of the ARPANET is several orders of magnitude greater than most HF nets, the rate of message injection into the HF net must be controlled in order not to produce damaging levels of congestion in the HF net.

3. The ARPANET does not send broadcast messages (i.e., each message must have a single destination) and therefore any multiple destination messages in the HF net must be blocked from entry into the ARPANET.
4. Since the ARPANET (and PRNET) will most probably be used as transit nets, a hierarchical addressing scheme should be used. If hierarchical addressing is used then, since multiple gateways enhance the survivability and reliability of the internetwork connection, the problem of multiple injections into the ARPANET arises. One solution would be to require the gateways to wait different amounts of time before injecting the message into the destination network. At the same time the gateways could monitor acknowledgement traffic or advisory messages sent by an injecting gateway to the other gateways in the HF net (acknowledgement traffic in the ARPANET is point-to-point and hence one gateway would not necessarily be able to receive an acknowledgement meant for another gateway). This scheme could lead to longer delays, however, and if the traffic into the ARPANET is not great then perhaps multiple injections should be allowed. Another solution, of course, is to specify the particular gateway to be used. However, HF propagation problems could result in a decreased probability of delivering the message to the ARPANET if this solution is used. The danger of swamping the HF net by multiple injections from the ARPANET to the HF net does not exist due to the reliable point-to-point nature of ARPANET traffic and resulting ability to select a particular gateway into the HF net.

Also, care must be taken to avoid infinite loops among gateways. This is a concern if the ARPANET is to be used as a transit net. A message could be delivered to a gateway to the ARPANET, transit the ARPANET and emerge into the HF net. The message (or copies of the message) could then arrive at another gateway into the ARPANET before it reaches its destination. To prevent this the message could be flagged as it transits the ARPANET. However, if the ARPANET were to become severed and several transits of pieces of the ARPANET had to be traversed, then this technique would have to be modified.

5. HF network protocols would need to be implemented. This would include protocols for accessing the gateway, network access techniques, time out periods (which may need to be modified before or after ARPANET transit), synchronization, error-control techniques, etc.

3.6.4 Cryptographic Considerations

Due to the conceptual nature of this paper the cryptographic considerations are limited to:

- a. Key Management
- b. Increased Overhead
- c. Red and Black Isolation

A probable method has been put forth on encrypting the message in Section 4 that would not impact the PRNET and ARPANET.

4.0 CRYPTOGRAPHIC ASPECTS

This section assumes that secrecy systems deal with baseband signals, defined here as unmodulated signals; this permits us to be concerned with the direct effect of a cryptographic device on a message and not with the radio or landline systems involved. In general, digital cryptographic devices add (modulo 2) an input clear-text bit stream to a pseudo-random key stream, producing a cipher-text bit stream. At the other end of the link, the cipher-text is again added (modulo 2) to the identical key stream, thereby retrieving the clear-text.

Compatible cryptographic devices need a common key in order to generate identical key streams. This key is the heart of the encryption process. A key stream is generated by inserting the key into a cryptographic algorithm. A worst case assumption in the cryptographic field is that the enemy has all the plans or even a copy of the cryptographic device you are using, only the secrecy of the key protects the message.

We shall consider the cryptographic aspects of the interoperability problem from the standpoint of both system commonality interoperability (Intra-crypto-net communication) and gateway interoperability (Inter-crypto-net communication).

4.1 Intra-Crypto-Net Communication

A crypto-net is a conceptual entity, the members of which are defined by their ability to encrypt and decrypt each others traffic with an identical key. Since we are dealing only with baseband signals, the concerns for communication within a crypto-net are Key Management, Overhead and Red/Black Isolation.

A crypto-net does not have to be limited to a system network. Allowing for the proper key management, synchronization techniques (overhead), and engineering design (Red/black isolation) the base-band signal could be encrypted in one system and decrypted in another.

4.1.1 Key Management

Key management is the process of distributing the proper keys to the intended subscriber's cryptographic device. Manual or on-line loading of the keys are two distribution methods. In the manual loading case, a "key gun" is plugged into the cryptographic device and the key passes through this physical interface. For on-line loading, the encrypted key is sent down the communication link, then decrypted and sent to the appropriate register in the cryptographic device for verification before replacing the current key.

Key management will be complicated if a given node has many secure systems, each of which are a member of a different crypto-net and use compatible key guns. An example of a potential problem would be Device A receiving Device B's key. Present key guns do not keep records of where they are to (or have) deposit(ed) the key, thus it is possible, by some human error, to put B's key in A. This may go undetected until an operator tries to read a "decrypted" message. Detailed accounting and key tagging methods will be needed to insure that the proper key gets to the proper device on each platform.

Encrypting the message and attaching an unencrypted (clear) header is one way to deal with secure message transfer from one network to another via a gateway (inter-system network transfer). A gateway need only change the header to conform to any intermediate system's protocol and not decrypt the message itself. If the message packet of the sending network exceeds the length of the receiving network, the message would have to be split into multiple packets. When the message is rejoined, it must not suffer a loss or gain of bits or the decryption process will not properly take place.

A concern with inter-system network transfer is key management. As stated earlier, members of different systems could be members of the same crypto-net, thus they need the same key. Encryption of the message and adding a clear header allows a gateway to remain a black^{*} device. Additional cryptographic protection could be added by further encrypting the message/header packet within a given system with a different key.

4.1.2 Overhead

Synchronization of key streams is required between two members of a crypto-net if they are to "talk" to each other. There are two different strategies for attaining synchronization; Message Indicator (MI) or Clock Start (CS). After the initial synchronization, the cryptographic devices send alignment bits at either set or random intervals to insure that the key streams are still aligned.

* Refers to encrypted data or areas that have encrypted data.

In the Message Indicator (MI) mode, part of the message header must contain information that aligns the pseudo-random key streams for the decryption process. The amount of overhead varies depending on the communication medium and device-synchronization strategy. Longer synchronization leaders are needed for noisy channels. The alignment of the pseudo-random key streams can be accomplished in a variety of ways. The additional overhead associated with cryptographic devices operating in the MI mode would have to be accommodated in the design of an inter-network system.

In the Clock Start (CS) mode, the need for a header is eliminated. The systems determine where in the key stream to start encryption or decryption based on the time of day, hence requiring accurate system-wide clocks. As an example, a key begins generating a pseudo-random stream at 0000Z, running at 1000 bps. If a message is sent after one hour, it would start to be encrypted with the 360001st bit of the pseudo-random key stream ($3600 \text{ seconds} \times 1000 \text{ bits/sec} + 1$). Upon receipt, the receive station would know the approximate time the message was sent. To determine the exact place in the encryption stream the message was added to, the receiving cryptographic device would have to search a "window". This would account for any clock offset between the two stations, propagation delays, and signal processing time (at both ends of the link). Once a correlation function threshold is exceeded, the proper place in the key stream has been found and the stations are synchronized.

Which method to use depends on the system and its operational concept. The trade-offs are: MI's synchronization overhead verses CS's accurate system wide clocks. If, for example, a system has few

transmitters and a number of receive-only (R/O) stations the CS method could be used since it allows R/O stations to come on-line without the transmitter(s) interrupting message traffic to transmit a synchronization leader. On the other hand, in a network that handles intermittent, packet-switched traffic the MI method might be better since the propagation delays, from packet to packet, vary greatly (i.e., the receiver would not know precisely when the packet was encrypted).

In the secure inter-system network case discussed in the key management section, the synchronization method used must be compatible with both networks. An example of a possible method is the transmitting station sending the receiving cryptographic device what time the packet was encrypted. This quasi-CS method could align the key streams as in the pure CS case but without the need for accurate system-wide clocks.

4.1.3 Red and Black Isolation

Tempest requirements are NSA standards for red/black isolation in DoD communication systems. These guidelines are for the communication systems themselves and for integrating a cryptographic device into the system. Tempest guidelines require the separation of non-secure and secure lines that process red and black data to insure message integrity. Physical separation and filtering of the red^{*} and black lines where these two data types are co-processed prevents compromising emanations. If red information of sufficient strength were to get on to the black lines, the whole concept of sending a cryptogram would be defeated. These emanations allow a crypto-analysis to recover the clear-text message.

*Refers to unencrypted data or areas that have unencrypted data.

As previously mentioned, an inter-system gateway could be a black device. As such, it could meet a less stringent set of isolation requirements than if it were processing red information.

4.2 Inter-Crypto-Net Communications

Communications between crypto-nets introduces some interesting problems. As already stated, differently keyed cryptographic devices cannot encrypt or decrypt each others traffic; hence the need for cryptographic gateways. These gateways would decrypt the incoming traffic from one network and then encrypt the message for the next network. The same problems covered in the previous sections exist in this area but are slightly different. Currently there are no digital crypto-net gateways available or in development within the DoD community.

4.2.1 Key Management

Inter-crypto network data transfer would involve decrypting and encrypting the message at each gateway. This method necessitates global key management among the networks involved so that the gateways have the proper keys to do the job. This encryption and decryption forces the gateways to be red devices.

4.2.2 Overhead

The synchronization technique of one network should not impact another network. The gateway would use and discard any associated overhead from the first network and would then use the alignment techniques of the second.

4.2.3 Red/Black Isolation

If the gateways of the inter-network systems process red information they will have to meet strict Tempest requirements. The possibility of compromising emanations exists in a cryptographic gateway, thus it would require strict Tempest controls as was discussed in Section 4.1.3.

5.0 COMPATIBILITY

Simultaneous operation of multiple communication systems on a single platform can cause operational problems. One system may interfere with another. An example of Electro-Magnetic Interference (EMI) problems in an LCC can be found in the communications evaluation of the Ground Launch Cruise Missile (GLCM). Because of EMI, the GLCM Launch Control Center's communications performance was rated marginal.

HF transmitter interference was the cause for the marginal performance not only in GLCM's HF receivers but also in the VHF and UHF-SATCOM radios and the Audio Intercommunication System (AIS). The AIS was directly affected by HF transmissions below 20 MHz. Performance of the radios, including the HF receivers, was degraded by the HF transmitter's harmonics. Interference also caused power supply shutdowns due to a power build-up on the associated cables.

The effectiveness of communications systems in a C² center will be impacted by the compatibility of the elements. Assessing the performance of individual systems in isolation may lead to excessive confidence of the centers overall capabilities. Since the antennas are in close proximity in the mobile environment, greater care should be exercised when integrating communications systems into the shelter to prevent these problems.

REFERENCES

1. Janes Military Communications, Janes Publishing Company Ltd., London, England, 1984.
2. E. Feinla and J. Postel, editors, ARPANET Protocol Handbook, NIC 7104, revised January 1978.
3. M.S. Frankel, et al., "Distributed, Survivable Command and Control/Army Data Distribuiton System/Packet Radio Testbed," SRI International, November 1982 - March 1985 (a series of six reports).
4. K.H. Kirchofer, "Key Management in Cryptographic Systems," International Defense Review, Vol. 13, pp. 1396-1398, 1980.
5. R.K. Miller, Jr., et al., Defense Data Network Subscriber Interface Guide, MTR-83W00133, The MITRE Corporation, August 1983.
6. R.D. Rosner, Packet Switching - Tomorrow's Communications Today, Lifetime Learning Publications, 1982.
7. C.E. Channon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol. 28, pp. 656-715, 1949.
8. F.G. Smith, Data Communications and the System Designer, UMI Research Press, 1979.

GLOSSARY

ACK	ACKnowledgement
ADCOM	Aerospace Defense COMmand
AFCS	Air Force Communications Service
AFLC	Air Force Logistics Command
AFSK	Audio Frequency Shift Keyed
AIS	Audio Intercommunication System
AJ	Anti-Jam
ALCC	Airborne Launch Control Center
ALCC	AirLift Control Center
ALCE	AirLift Control Element
ALL	ALLocation
AM	Amplitude Modulation
AME	Amplitude Modulation Equivalent
ANMCC	Alternate National Military Command Center
ARPANET	Advanced Research Projects Agency NETwork
ARQ	Automatic Repeat ReQuest
BB	Black Box
BBN	Bolt Beranek and Newman
bps	bits-per-second
CCEC	Command Control and Engineering Center
CCT	Combat Control Team
CDMA	Code Division Multiple Access
CINCUSAREUR	Commander IN Chief United States ARmy Europe
COMM COM	Communications Command
CRC	Cyclic Redundancy Check
CS	Clock Start
CW	Continuous Wave

DARPA	Defense Advanced Research Projects Agency
DCA	Defence Communications Agency
DDN	Defense Data Network
DEA	Drug Enforcement Agency
DoD	Department of Defense
DPSK	Differential Phase Shift Keyed
DSB	Double Side Band
EAM	Emergency Action Message
EMI	Electro-Magnetic Interface
EPR	Experimental Packet Radio
EUNIEF	EUCOM Nuclear Interface Element - FASTBREAK
FAA	Federal Aviation Administration
FAC	Forward Air Controller
FAX	Facsimile
FCC	Federal Communications Commission
FDM	Frequency Division Multiplex
FDMA	Frequency Division Multiple Access
FEMA	Federal Emergency Management Agency
FM	Frequency Modulation
FOC	Final Operational Capability
FSK	Frequency Shift Keyed
GLCM	Ground Launch Cruise Missile
GWEN	Ground Wave Emergency Network
HBH	Hop-By-Hop
HF	High Frequency
I/O	Input Output
IMP	Interface Message Processor
IP	Internetworking Protocol
IRR	Integrated Radio Room
ISO	International Standards Organization
JCS	Joint Chiefs of Staff

LCC	Launch Control Center
LF	Low Frequency
LPR	Lowcost Packet Radio
LSB	Lower Side Band
MAC	Military Airlift Command
MEECN	Minimum Essential Emergency Communications Network
MI	Message Indicator
MILNET	MILitary NETwork
MILSTAR	Multi-service Satellite Communications System
MS	Minimum Shift
MSG	MeSsaGe
NCP	Network Control Program
NSDD	National Security Decision Directive
NVT	Network Virtual Terminal
PAC	Pacific Air Command
PACAF	PACific Air Force
PCM	Pulse Code Modulation
PLT	Pending Leader Table
PN	Psuedo-Noise
PRNET	Packet Radio NETwork
PRU	Packet Radio Unit
R/O	Receive Only
REQALL	ALLocation REQuest
RFNM	Request For Next Message
SAC	Strategic Air Command
SACDIN	Strategic Air Command DIgital Network
SATCOM	SATellite COMmunications
SRI	Stanford Research Institute
SSB	Single Side Band
TAC	Terminal Access Controller

TAC	Tactical Air Command
TACAMO	Take Command And Move Out
TADIL	Tactical Digital Information Link
TALO	Tactical Airlift Liason Office
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TEP	Terminal Emulation Processor
TIU	Terminal Interface Unit
TSEC	Transmission SECurity
TTY	TeleTYpe
UHF	Ultra High Frequency
USAFE	United States Air Force Europe
USB	Upper Side Band
USEUCOM	United States EUropean COMmand
USN	United States Navy
VA	Veterans Admisistration
VHF	Very High Frequency
VLF	Very Low Frequency
wpm	words-per-minute
WWABNCP	World Wide Airborne Command Post